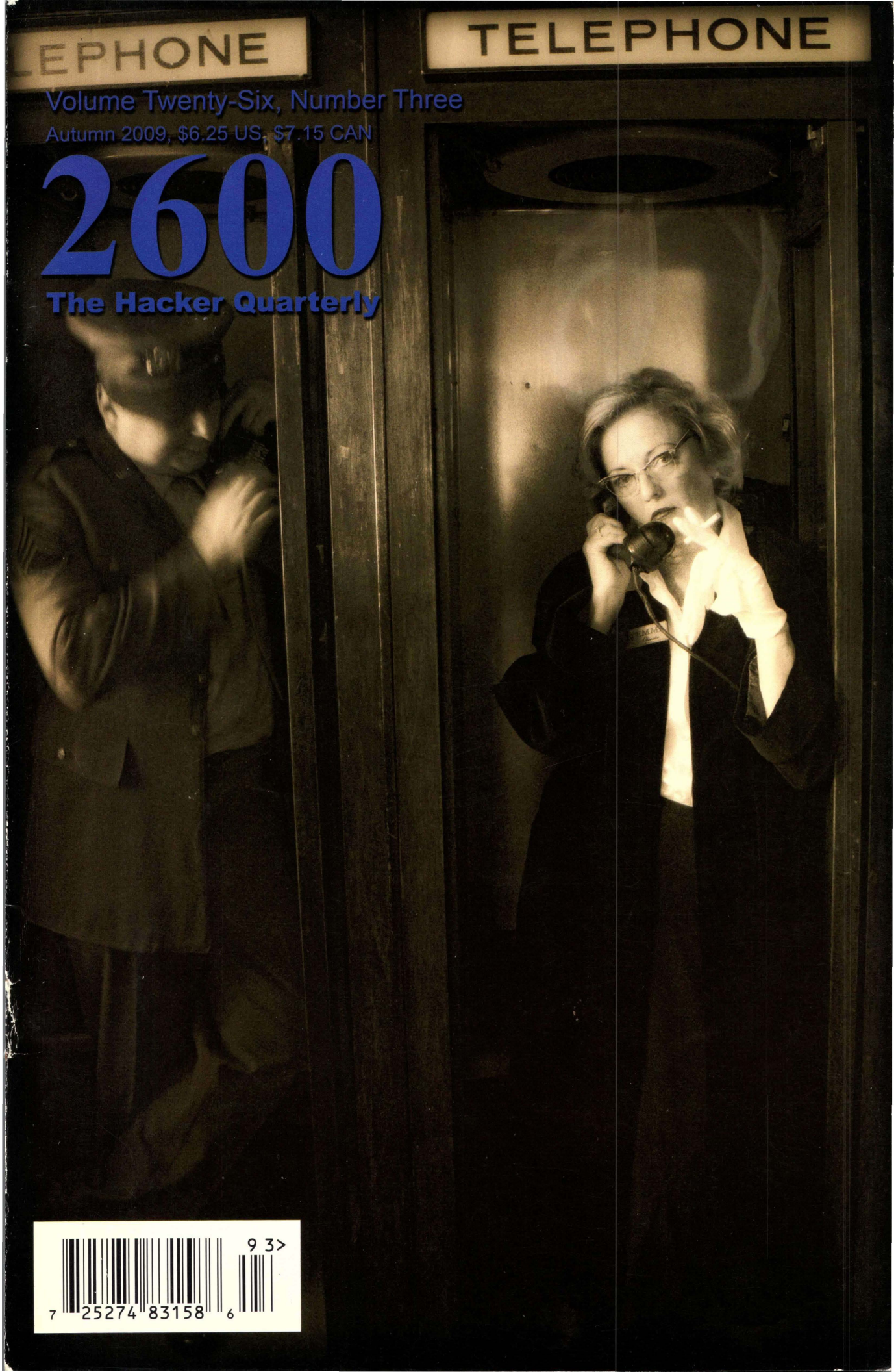


Volume Twenty-Six, Number Three
Autumn 2009, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly

9 3>
7 25274 83158 6

Payphones in Exotic Places

Guatemala. One of the typical phones found throughout the country.

Photo by Gary Davenport

Burkina Faso. This rather dusty phone was found in the city of Ouagadougou. Note the symbol for international calling: one flag connecting to another.

Photo by M J

Rwanda. Seen in the departures area of the Kigali Airport. (It didn't work, incidentally.)

Photo by Jeffrey Mann

Mauritius. This brightly colored model that takes both coins and cards was discovered beside the Pereybere Beach in Pereybere.

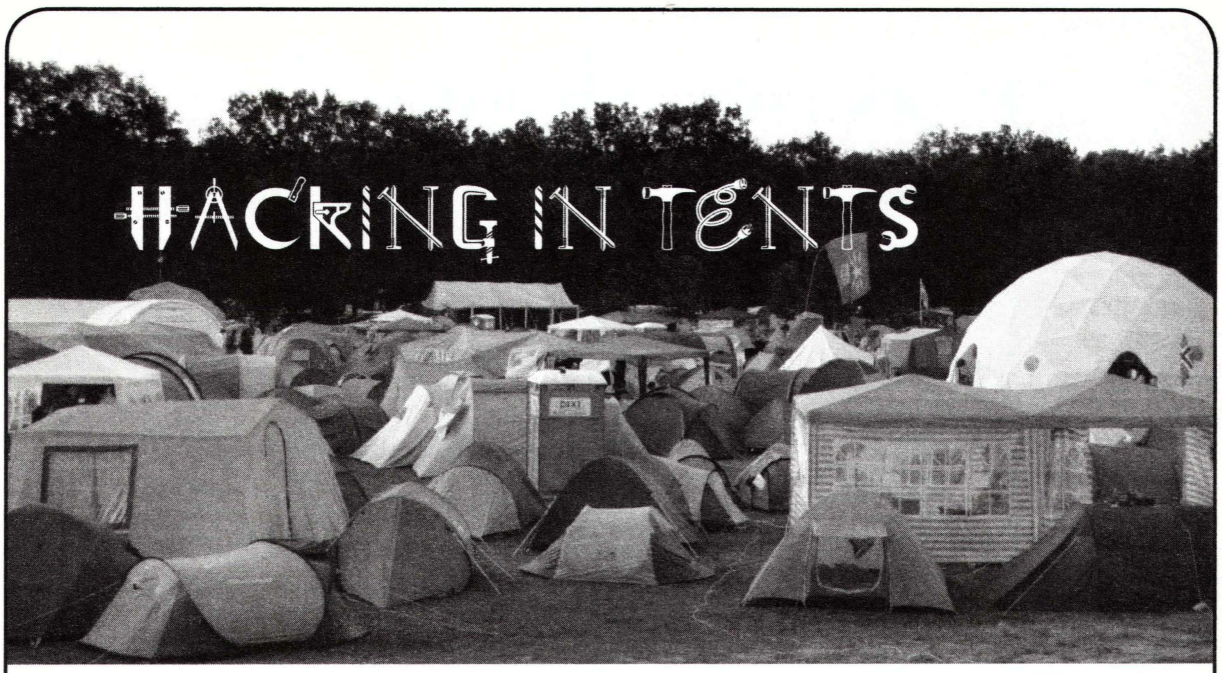
Photo by Scott Brown

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

FORENSICS

Hacking In Tents	4
Exploiting University Students using Rogue Access Points	6
Catching a Laptop Thief/WiFi Hacker	8
Attacking a Blind Spot	9
How to Almost Hide Your Digital Identity While Port Scanning	11
TELECOM INFORMER	13
Hello! Google Calling	15
Post-Apocalyptic Communications	16
Roll Your Own Hive-Mind	17
Free DirecTV on Frontier	18
Free Trials - Avoid Giving Out Your Credit Card Number	19
If You Can't Stand the Heat, Hack the Computers! (Part 2)	20
HACKER PERSPECTIVE: Johannes Grenzfurthner	26
Granny Loves Linux!	29
Cracking WPA - PSK	30
HACKER SPACES	33
LETTERS	34
Hard Disk Encryption, No Excuses	48
Microsoft, Please Salt My Hash!	49
How to Get Free Loans From American Express	51
TRANSMISSIONS	52
SSL DNSSEC	54
Tethering the Samsung SCH-R450 on MetroPCS	57
"Borrowing" the CustomInk.com Vector Library	59
Hacking Your Hospital Bed	60
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

changed priorities ahead



It was another historic summer.

For a good number of us, the accomplishments mirrored those of previous years. For many others, it was something entirely new. For the hacker community at large, the summer of 2009 represented a reaffirmation and a significant expansion into brand new territory.

The concept of a hacker camp was first realized in 1993 as Hacking at the End of the Universe (HEU) was held in the Netherlands. There, for the first time, people in our unique community figured out a way to build a mini city in the middle of the wilderness, complete with power and connectivity, dedicated to the world of hacking and innovation. It was enough to inspire us to move ahead with the first HOPE conference a year later in New York. That, in turn, was the first American conference to draw over 1,000 attendees. History was made.

Another Dutch hacker camp took place four years later in 1997, known as Hacking In Progress (HIP), held in conjunction with the second HOPE conference (Beyond HOPE). Then, the German Chaos Computer Club put together the first German hacker camp in 1999. From that point, HOPE conferences in New York were held during even years and alternated with the European hacker camps which, in turn, alternated between Germany and the Netherlands during odd years. The Germans held Chaos Communication Camps in 2003 and 2007 while the Dutch held Hacking At Large (HAL) in 2001 and What The Hack in 2005. Add to that list this year's presentation of Hacking At Random (HAR). Apart from a seemingly neverending supply of clever names, the spirit of these events also seems limitless. Not to mention contagious.

For this year also saw something brand new. The first ever hacker camp in the United States became a reality in early July. ToorCamp took place in the middle of Washington State at, of all places, the site of a former nuclear missile silo. It wasn't nearly as big as the European counterparts, but it was every bit as significant. Just as we once thought it would be impossible to hold a massive hacker conference in the United States, we also believed pulling off a hacker camp most certainly would never happen in this country. We're happy to have been proven very wrong.

With a little ingenuity and a lot of spirit, all kinds of events in the most unlikely of locations can be successfully coordinated. To have hundreds of hackers occupying a site that once could have been a trigger to the end of the world is both surreal and inspirational. We've gotten used to the Germans having camps and conferences at old military airports or former communist training centers. How is it possible to measure up to *that* level of coolness? This summer, a big step was taken in achieving parity. Not only was ToorCamp held in an amazing setting, but the sheer amount of responsibility the attendees displayed rivaled that of the overseas conferences, where *everyone* is a volunteer and security is relatively seamless and transparent. The only way an outdoor hacker conference can possibly work in a place like an old missile silo is if everyone works together and makes sure safety is a

priority in a potentially hazardous environment. With this accomplished, there is almost no limit to the potential of where the next outdoor hacker event might take place in the States. Now that we know it can be done, we have a whole country of really neat places to hold the next one in. Let's hope the inspiration from this event leads to many more of them.

Of course, we expected greatness from HAR and there was certainly no shortage of that. Four full days of talks and gatherings including people from so many different nationalities made it truly impossible to be bored. The time flew by incredibly fast. Naturally, an event of this nature has a great number of challenges and all of them were tackled by a very dedicated group of people, many of whom had arrived days before and wound up staying days later to ensure that everything worked out. A few of the tasks included keeping the wired and wireless connectivity going, managing the actual infrastructure of plumbing and power, dealing with the steady curiosity of the media and the authorities, coordinating the speaker schedules, even running two separate phone systems. Yes, the camp had both a DECT wireless telephone system and its own GSM network, each allowing attendees to use their phones to call others on site for no charge. An FM radio station ran around the clock and captured the spirit of the proceedings with all sorts of interviews, news coverage, and music, every bit of which was done in a professional and fun manner. There really seemed to be no end to the innovation and fun that was possible at this event.

While this type of magic has started to become almost routine for those of us involved in the hacker community, we do need to have this reinforced on a regular basis. With every one of these milestones, more new people get involved and become inspired. This is essential in order for our community to continue to flourish. Having the same people doing the same thing, no matter how great it may be, would still be a form of stagnation. At all costs, we must avoid anything that erects barricades to new participants. And those new to the scene must try and learn from the experiences and mistakes of those who've been involved in the past.

The kinds of conferences we've seen in ToorCamp and HAR (and we'd like to assume our own HOPE conferences) are significantly different from those events that treat their attendees as a mere audience. Some people prefer it that way because they don't really have to do anything except pay their admission fee and follow the instructions. The people who run such conferences are very different and separate from those who attend and the hierarchy is painfully evident to all. A good hacker conference, however, has only a slight difference between those organizing the event and those who attend with no previous involvement. Oftentimes, the latter turn into the former, sometimes in the course of the event itself. This is how great things are possible - with the potential for innovation, change, and something completely unexpected and unanticipated.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2009. Annual subscription price $24.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	52,250	50,000
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4,893	4,687
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	44,864	42,890
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	49,757	47,577
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	216	183
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	2,277	2,240
E. Total free distribution	2,493	2,423
F. Total distribution	52,250	50,000
G. Copies not distributed	0	0
H. Total	52,250	50,000
I. Percent Paid	95	95

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

Exploiting University Students using Rogue Access Points

By Anonymous

A rogue access point is a wireless access point that has been installed on a network without permission. It could just be an access point that was set up by a student or faculty member to provide wireless access in an area where none existed. Or, it could have a malicious objective like a man-in-the-middle attack where sensitive information could be stolen. Several years ago, my university installed 802.11 wireless access points throughout campus. Unfortunately, the wireless is set up in a way that allows for rogue access points to be brought onto the network easily. The focus of the paper is explaining how rogue access points can be used in the university environment to exploit students and faculty workstations to gather sensitive data. First, I will examine the vulnerability. Second, I will describe the different attack vectors where one could exploit the vulnerability. Lastly, I will describe ways to collect sensitive data and how one could use the captured data.

As I mentioned, the university installed 802.11 APs around the campus. All of the access points communicate to the end devices with the same, unsecured SSID. By unsecured, I mean the access point is not secured with static WEP or WPA keys, or an enterprise authentication solution. In a corporate environment, you will find secured access points because the corporation is trying to keep unauthorized persons out of their network. However, in a university setting, they are trying to provide usability on their wireless so students and faculty can get on it without trouble. To allow usability, the university moved the authentication from the wireless protocol itself to a web based splash page asking for credentials. When a user connects to the wireless, their web browser is automatically redirected to a SSL secured splash page where they are required to login to get access to the network. There is no client-side software to this login and it is based off of the machine's MAC/IP address. Once logged in, they have access to the network and Internet.

My university also sells laptop computers that come customized with common settings and shortcuts that the student would find useful. One of these settings is adding the university's wireless network. This will allow any student who buys one of these laptops easy access onto the university's wireless network without him/her having to setup anything. This means that every laptop purchased from the student stores will automatically be looking for and trying to connect to an unsecured access point.

The laptops purchased at the student stores are not the only computers automatically looking for and trying to connect to the university's unsecured access point. Any laptop that has ever connected to the wireless will now have that wireless connection in its wireless profile. If the user is running Windows and is using Wireless Zero Configuration (WZC), then every wireless network ever connected to will be in the preferred networks list. The higher the connection is on the list, the higher its priority. For example, if the user connected to the university's wireless in 2008, and in 2009 connected it to their new wireless router at home, then the laptop will connect to the university's SSID even if it sees their new wireless router as available. Since a lot of university students live in dorms their first year, the probability of having the university's SSID near the top of their preferred networks list is high.

If you merge the ideas from the last three previous paragraphs, then you end up with the vulnerability. First, the APs are not secured. This means that a miscreant can create a rogue access point and everyone will automatically connect to it as though it was owned by the university. Second, all student laptops (and specifically those bought at the student store), will be actively looking for the university's wireless connection. Even further helping the miscreant is that the laptops bought from the student store list the university's wireless connection as the preferred connection. This means that they will connect to the university's wireless network even when they are not at the university. To gather information using a rogue access point, the miscreant has to figure out where students are when not at school. A good place to start would be their residence.

The first attack vector is apartment complexes. There are tons of apartment complexes around my university, housing 1000s of people. The majority of the people living in these apartments are students at the university. A good majority of university students have laptops with the SSID of university saved as

a wireless profile. If someone sets up a rogue AP, then anyone in proximity will automatically connect to it. The number of users who will connect to the rogue AP is based on how high the university's wireless profile is in the preferred network connections list. The longer one leaves the rogue AP on, the more users that will connect to it. More users will also connect to it when their computer is restarted and looks for available wireless connections. Again, if the university's SSID is high in the preferred connections list, then it will connect to it if it sees it available. I will call this the most effective method because the miscreant will not be seen, and will never have to hide any of their equipment. This is also the setup where one could have the most equipment. Imagine three or four rogue APs each with high gain antennas positioned to pick up the most users.

The second attack vector is dormitories. My university did not extend the wireless throughout the dormitories, but instead installed APs only in the lobbies and study areas (basements). This means that above the basement, once the signal bleeds off, there are 100s of laptops looking for the university's SSID. If a miscreant sets up a rogue AP, one could easily grab a bunch of users instantly. In reality, one could just put the rogue AP in a car and mount the antennas on the roof. This would not provide the depth of coverage as the first method, but would be much easier to implement.

The third attack vector is on the campus. If the miscreant is brave, and believes that the data he/she wants to collect is on the physical campus, then he/she could setup a rogue AP in the ceiling using a laptop by itself, or the combination of a laptop and external AP. The issue of long term power is easily solved. All of these new "smart classrooms" have electrical outlets for the projectors above the ceiling tiles. Not only will the AP run forever, but it is hidden from view. The downside to this is that if the university is running any kind of rogue AP detection, and actively monitors it, the rogue will be found. However, the value of the data one could potentially gather might outweigh the risk. The primary reason for running a rogue at the university is to capture faculty data.

Along the same lines as putting a laptop in the ceiling, one could put it in a book bag wired to a UPS. This would only last for a couple hours (depending on how much weight in batteries one wants to deal with), but is mobile and has little chance of someone ever finding it. Here is a scenario. Pretend you're a student and go into a large lecture hall. If you find a hall where they teach an IT subject, then the majority of the students will bring their laptop. Power up your book bag, and hope that they connect to you. If you get to class before they do and get your book bag powered up, then there will be a high probability they will connect to you because your device will have the best signal strength.

After a miscreant has set up the rogue access point, they can start collecting data. First, one would start by simply sniffing the traffic to determine which websites are being visited the most. From there, a local web and DNS server running on the laptop could be setup to serve phishing pages matching those sites. The reason for the phishing pages is that most credentials, at least ones that have any real value, will be sent across SSL. Creating a phishing site will guarantee the credentials, but may arouse suspicion if one doesn't pass them to a believable error page or if they never get the real website. To get around this problem, a cron job could be used.

Cron is a job scheduler for Unix/Linux operating systems. One could create a job that rotates the DNS entries between the IP that points to the phished and real website. In terms of believable error pages, Facebook has a habit of going into maintenance mode and only prompting a user that they are in this mode once they try to log in. A phished Facebook page throwing the user to the fake maintenance message would be highly effective.

Another option is to phish the university's initial wireless splash page that requires logon. The credentials for the wireless are also what the student uses to access their email and other university websites. The first obstacle for the miscreant is getting onto the wireless network so that he/she can serve Internet access and not arouse suspicion. I mentioned before that wireless access is based off of the laptop's IP and MAC address. Simply sniffing the wireless will yield someone who is connected and possibly authenticated to the wireless. Then, by cloning their IP and MAC address, one is now logged into the wireless as someone else.

Now that the miscreant has phished some credentials, there are several things one can do with them. If he/she captured the credentials for the wireless splash screen, one now has access to the student's e-mail. Their e-mail address is the gateway to getting passwords to numerous other sites. For example, Facebook has a "forgot your password?" page that will send an email to reset your password. There is a good chance this email will go to the student's university email address. For any captured credentials, there is a chance that the user uses the same password for other sites. For example, if one captures their Facebook password, then one might also have their MySpace password. The issue would now be guessing their username.

That's all. I have no insightful conclusion. Go have fun!

Shouts to all who have supplied me with the resources to learn

Catching a Laptop Thief/WiFi Hacker

by Douglas Berdeaux
douglas@weaknetlabs.com

Years ago, when I first saw the movie *Track Down* (*Takedown*), I was impressed. I thought it was a cool movie and have been bashed several times for such a statement. I even heard Kevin Mitnick once say that the movie "sucked" in an interview on a radio show. But out of all of the cheesy hacker movies, I felt that it had the coolest feel to it. The part in the movie were Shimomora is in the van searching for Mitnick gave me an idea. I could possibly do the same thing with MAC addresses and the aircrack-ng suite. With a cheap wireless card, a free light-weight coding language, and some patience, I too could be trolling in the back of a van. But again, searching for a MAC address and not a MIN or ESN (yet).

Now, I don't own a van, I don't have friends, and I wouldn't really care if someone cracked my network security. *But* I would care if, say, I had a laptop stolen from me in a mugging, or from my house when I wasn't home, etc. I could then check the MAC address I wrote down of the internal WiFi card, or on the side of the laptop box, for even better evidence, and search for it! This would, of course, only going to work if the thief weren't smart enough to change the card, leave the state, etc. If you think of this situation with mathematical crime statistics and probability, it's most likely the case.

Windows, and any other OS that has a network manager-like client running, will either be connected to an AP listed in your preferences, or will be probing for APs in your list. Also, it will be actively sniffing for surrounding APs to suggest them to you, as if its life depended on it.

When a client probes for a preference AP, the data sent via WiFi will be visible to anyone in the surrounding area equipped with the proper setup. By this I mean anyone with a card that can be set to "monitor" mode by the user and running airodump-ng while channel hopping.

I have had a lot of experience with WiFi cards, vendor types, and driver issues in the labs here and have found that almost any card that is detected by a Linux/Unix flavor OS can be set into "monitor" mode for sniffing. This means that the card has the ability to "sniff" surrounding APs, to list them for you to connect to, but does not always mean it can "inject" fabricated packets. You would want to inject fabricated packets to deauthenticate a user in order to grab a WPA/WPA2 handshake, which would allow you to attempt to crack, with a dictionary file or hash file, the login info using aircrack-ng or cowpatty 4.0+.

But in our case, we are simply sniffing, so any old card should do the trick. You can skim forums where they talk about this sort of thing, like wireless security, to find out which cards are best for the job. I would first recommend the Remote-Exploit forums, as they have almost benchmarked every card on the market for their sniffing capabilities! They have a lot of experience with wireless hacking and are first to point out a vulnerability, or code to exploit it.

Once you have a good card, you're ready to start searching for your cracker/laptop thief! First, boot up into a Live Linux disk like WeakNet Linux Assistant. Then connect to your wired internet and download the catchme-ng tarball here: `http://weaknetlabs.com/➥code/catchme-ng/` Now disconnect and save the tarball for future use on a flash drive. Put your wireless cards down and kill network-manager. By typing `ifconfig`, you can list the cards that you have "turned on." Then `ifconfig ➥ <cardname> down` will turn them off temporarily. This can also be accomplished by killing network-manager with killall network-manager. Usually that turns off all of the network cards in one fell swoop.

Now we want to set our wireless card to monitor mode and turn it back on. Type `iwconfig` to list all of your wireless cards. Type `iwconfig <cardname> mode monitor` to set it to monitor mode. This is where you can determine if your card is capable, with the drivers included in your OS, of going into monitor mode. The OS isn't very embarrassed at this point to cry out! If successful, turn the card back on with `ifconfig <cardname> up`, and start airodump-ng with the --write to file option. Make sure you remember what your current working directory is and where you are saving your files to. I'd suggest changing directories and just saving them in /tmp.

Once started, fire up catchme-ng and click on the "..." button to find your "dump file" created by airodump-ng. Then select the MAC address you want to hunt for and click start. If your prey (MAC you're searching for) comes within your wireless card's sniffing range, you will see it. A loud siren sound will play, and a box will pop up saying "I've found the MAC

specified." Now, simply toss your laptop into your car/bookbag/etc. and walk/drive/bike around your neighborhood with headphones on in search of your machine. If you find the machine, you can now set up nearby and zero in even closer by watching the "PWR" field of airodump-ng. You can see the "power," or pretty much the range, of the client that is either "probing" for, or connected to, an AP.

And that's all there is to it, really. Imagine the possibilities of these applications in parallel. Law enforcement can find the MAC address of a stolen laptop. You can pinpoint, with quite good accuracy, who broke into your network by comparing the logs of MAC addresses with your very own addresses and the foreign address being specified as the "prey." You can search for anything with a MAC address. If you aren't sure how to find a MAC address in your logs, you can simply write a shell script to frequently check your LAN for new MAC addresses and dump them to a text file, without creating doubles or overwriting previously seen MAC addresses. Here is an example of such a LAN-nanny:

```
sudo ettercap -Tpi eth0 // // -k
➥ 1.txt -s q && cat 1.txt | awk
➥ '{print $2}' >> 2.txt && cat
➥ 2.txt | sort -u > MAC_List.txt
```

This relies on Ettercap to find the MAC addresses on your LAN. This is a good choice because it's fast, and speed counts when you know that some wireless security measures are flawed when it comes to ARP requests. If we were to use the basic ARP program `arp -a`, it would take a bit longer.

What the above script actually does, in plain English, is "run Ettercap, use text mode, in non-promiscuous mode (so there's not a bunch of packets flooding the screen), use interface eth0, ARP for all clients on LAN and make text file 1.txt with results, print each line in 1.txt but only the MAC addresses column and append it to 2.txt, print every line in 2.txt sorting out the duplicates and spitting all of the unique MAC addresses into the text file MAC_List.txt." Now simply make this run every, say, 5 or 10 minutes or so. ARPs can seriously bog down traffic, of course, so maybe less often would be recommended.

Another application of the program would be to create a game to with your friends to wirelessly search for them! The program is not biased and you can specify even an ESSID that you once used and have fond memories of. There are endless possibilities!

Attacking a Blind Spot

by Tim Kulp (cloak13)

scotoma *n.* A spot in the visual field in which vision is absent or deficient.

Information security is full of scotomas. To find one, look no further than the network printer. Modern printers are no longer merely ink cartridges with a network card; they are document management systems with large memory stores and direct server access. Using unsecured network printers, you can own and disrupt a network resource that is critical for most business functionality.

Why a printer?

Enterprise/business computers have many checks and policies to monitor information coming from and going to them with devices like proxy servers and firewalls. Printers, on the other hand, do not access the web or even other computers; they only receive instructions to print and therefore do not need these various checks, right? Many modern network printers have management features that can be accessed via a web browser or telnet, which means that ports 80, 443 and 23 are open by default. Too often, IT professionals simply plug the printer in and point computers to it. They are ignoring the security implications of treating a printer as a "receive only" device.

A quick browse of the Ricoh or HP printer websites reveals that modern printers are capable of much more than just putting ink on various paper sizes. Today, printers have hard drives, access to network storage, and email, which translates to broadcasting data and not just receiving it.

Attack 1: Building your zombie (scanner) army

You have scanned your network to find systems with open ports using a tool like Nmap or HPing2 (for this article, we will be using Nmap). A system is returned with ports 515 (Printer/LPD), 631 (IPP) and 9100 (Jet Direct) open. These ports are the main PDL (Page

Description Language) data stream ports. PDL is the command language network printers use to know how to draw the document that they are trying to print. Having these ports open is a sure indicator that the device is a network printer. If you are still not sure, you can always run: `nmap -o [target IP address]`

The -o modifier tells nmap to determine the operating system of what you are scanning. If the device is indeed a printer, then you can expect something like "HP LaserJet 4050/4200/4600/5100 (JetDirect) printer," which tells you that the network printer in question is an HP LaserJet and could be a 4050, 4200, 4600 or 5100 model. This is great information to start looking for vulnerabilities, but for this attack we are only delivering a scan through our printer.

Letís get this printer working for us. Using the following command in nmap: `nmap -sI [printer IP address] [target IP address]`

The printer (now our zombie system) will scan the target for port information. This is called an idle scan or a zombie scan because, while you are executing the scan, another system tunnels the requests for you. This particular scan is useful when you know an IDS or IPS system will be logging scan activities. The IDS/IPS will record the scanning system's information which, when using a zombie scan, will be the zombie device (in this case, our target network printer). This type of scan is great for hiding your computer's identity while still retrieving useful and accurate port information from the target.

Attack 2: Killing trees, blocking business

While a zombie scan can be useful, you can do a lot more with an unsecured printer. Using just the address of the printer and telnet, you can send print jobs to the network printer. Using telnet and an unsecured printer, we are going to launch a DoS attack.

Connect to the printer via telnet: `open [target IP address]:9100`

This will open a telnet connection to port 9100, the port that receives all the PDL commands that we introduced earlier in the article. Type whatever you would like and press Crtl-] to send the command to the printer. This will cause the printer to print the text that you typed before hitting Ctrl-]. With a little scripting skill you can build an automated process that will print random strings, causing a tremendous waste of ink and paper as well as clogging the print queue and thus preventing other users from being able to print.

Another way to do this same attack is to connect to the printer via a web browser. As an example, you could type the following into the address bar of your web browser: `http://[printer IP address]:9100`

Notice we are connecting to port 9100. This connection will cause the printer to spit out an HTTP request. If you get creative with a tool like Fiddler, you can craft your own HTTP commands and flood the printer with HTTP GET requests. Each GET would be printed out, again causing the print queue to be flooded with bogus print requests.

But wasting paper is not the only DoS we can perform. Using telnet, you can change settings on an unsecured printer by connecting to port 23. You can use this connection to reset the Administrative Password, change the user time out, and a ton of other mischievous things. We will walk through a quick scenario that will get the printer's hostname using telnet and an unsecured HP 4050n printer.

Telnet into the printer using a standard telnet open connection command: `open [target printer's IP address]`

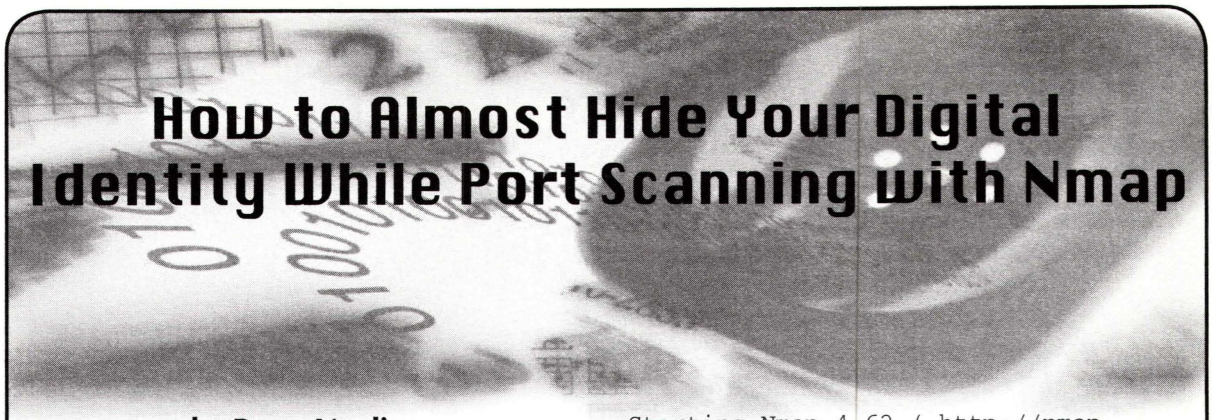
If the printer is unsecured, you will not be prompted for a username or password. After gaining access to the printer, type "menu" and hit enter. This will return the control menu. To get the hostname, select option 2, for "TCP/IP Settings," then select option 1, for "Main TCP/IP Settings." This will return all of the general TCP/IP settings, including hostname, IP address, subnet mask, etc... You can change the IP address here to create a simple, but temporary, DoS attack. As soon as network administrators realize no one can print to the specific printer, the changed IP address will be discovered and corrected. Whether or not the printer will then be secured is another story.

Return to the main menu and browse the other options to get a complete picture of all the settings you can manipulate. Many of these settings, with slight changes, can cause major disruptions in the printer;s operations or be other routes to a DoS attack.

Conclusion

The few examples in this article are simple attacks for standard network printers but can be used as a basis for more sophisticated attacks against robust printing systems. As printers improve in capabilities and features, new security issues arise. Imagine the security concerns of a "document management solution" printer, or of a printer tied directly to the company's Exchange server. If left unsecured, what kind of attacks could be used to compromise the connected systems? Like many non-computer devices, network printers are often forgotten in security audits and analysis. Keep this in mind during your next penetration test project. By targeting network printers, you can leverage a powerful network resource while operating in a very large security blind spot.

How to Almost Hide Your Digital Identity While Port Scanning with Nmap



by Bryce Verdier

For people in the know, port scanners are double-edged swords. While they give System and Network administrators the ability to scan for unwanted holes in their firewalls, servers, and computers, they also give malicious Internet users the ability to do the same thing and are usually the first tool a would-be intruder uses to find a way into a network. One of the most well known port scanners is Nmap. Nmap runs on Linux, FreeBSD, Mac OS X, Solaris, Windows, and more. So chances are that, no matter what OS you're running, you can run Nmap on it.

Disclaimer: Just because you're about to learn a new tool today, does not mean that you should go straight to work or school and just start scanning every computer in sight. This is a real good way to make the network administrators very angry. So be courteous; if you do not own the computer you're about to scan, get permission. And this is for educational purposes only, obviously.

I am quite sure that some of the people reading this article are more adept with this tool than I am. (If you're not, then I would recommend you spend some time with it before continuing with this article... or not.) For those who don't know, Nmap has the ability to change its scanning IP, and do the same trick with a group of IPs, or decoys, as the manual calls them. So for everyone who lives by their firewall logs, you might want to start keeping a closer look at your logs concerning port scans, because that IP that is scanning you is probably not the IP that you think it is.

From the manual, there are two arguments that I will go into in more depth: -S and -D. -S has the explanation of, "-S <IP_Address>: Spoof source address." And -D is described as, "-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys" (notice no space between the comma decoy1 and decoy2). If you do use "ME," you will put in your computer's IP address as part of the cycle of decoys. I do not know if you would want to do this, but maybe you do. Anyway, let's see some of these configurations in action:

```
$ sudo nmap -e eth0 -P0 -S
➥ 12.24.36.48 -A -T4 192.168.1.27
Starting Nmap 4.62 ( http://nmap.
➥ org ) at 2009-01-15 00:13 PST
Warning: OS detection for
➥ 192.168.1.27 will be
➥ MUCH less reliable
because we did not find at least
➥ 1 open and 1 closed TCP port
All 1697 scanned ports on mythbox
➥ (192.168.1.27) are filtered
MAC Address: 00:14:BF:5B:2D:5C
➥ (Cisco-Linksys)
Too many fingerprints match this
➥ host to give specific OS details
Network Distance: 1 hop

Nmap finished: 1 IP address (1 host
➥ up) scanned in 36.634 seconds
```

This is just to show you what I typed at the command prompt, so you can see how to use the -S argument and what to expect as possible results. As I said above, -S is to spoof the IP address of the hosting machine, which I have set to spoof as 12.24.36.48. However, I have a couple more arguments thrown in for good measure. First the "-e" this is telling Nmap which network card to use. Generally, Nmap knows which card to use, but I've decided to use it here to be explicit. The next extra argument is "-P0." This is to tell Nmap not to ping the host, as Nmap likes to ping before scanning to make sure the host is online. Now that we've gone over the boring stuff, let's look at some firewall logs.

```
Jan 15 00:13:01 mythbox IN=eth0 OUT=
MAC=00:14:bf:5b:2d:5c:00:13:d4:
➥78:18:c6:08:00 SRC=12.24.36.48
DST=192.168.1.27 LEN=44 TOS=0x00
➥ PREC=0x00 TTL=40
➥ ID=63097 PROTO=TCP
SPT=43468 DPT=1383 WINDOW=1024
➥ RES=0x00 SYN URGP=0
Jan 15 00:13:01 mythbox IN=eth0 OUT=
MAC=00:14:bf:5b:2d:5c:00:13:d4:
➥ 78:18:c6:08:00 SRC=12.24.36.48
DST=192.168.1.27 LEN=44 TOS=0x00
➥ PREC=0x00 TTL=47
➥ ID=56142 PROTO=TCP
SPT=43469 DPT=722 WINDOW=4096
➥ RES=0x00 SYN URGP=0
```

This output shows the results the command above has on my iptables firewall log. If you look in the screen shot on each line you'll

see: "SRC=12.24.36.48" which is the exact IP we set from the command line. We know this works with a single IP address, but what about multiple IP addresses?

```
$ sudo nmap -e eth0 -P0 -D 1
➥ 2.24.36.48,3.6.9.12,5.25.1
➥ 25.250 -A -T4 192.168.1.27
Starting Nmap 4.62 ( http://nmap.org
➥ ) at 2009-02-15 00:33 PST
Warning: OS detection for
➥ 192.168.1.27 will be
➥ MUCH less reliable
because we did not find at least
➥ 1 open and 1 closed TCP port
Interesting ports on
➥ mythbox (192.168.1.27):
Not shown: 1693 filtered ports
PORT STATE SERVICE VERSION
80/tcp open http lighttpd 1.4.15
631/tcp open ipp CUPS 1.2
6543/tcp open mythtv?
6544/tcp open mythtv?
MAC Address: 00:14:BF:5B:2D:5C
➥ (Cisco-Linksys)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9
➥ - 2.6.12 (x86)
Uptime: 0.031 days (since
➥ Wed Jun 13 20:11:22 2007)
Network Distance: 1 hop

Nmap finished: 1 IP address (1 host
➥ up) scanned in 138.657 seconds
```

Just like the first command, we start by Nmap telling it which network card to use and, instead of just specifying one IP address, we specify three IP addresses: 12.24.36.48, 3.6.9.12, and 5.25.125.250. Now let's take a quick look at our iptables log and see what happens.

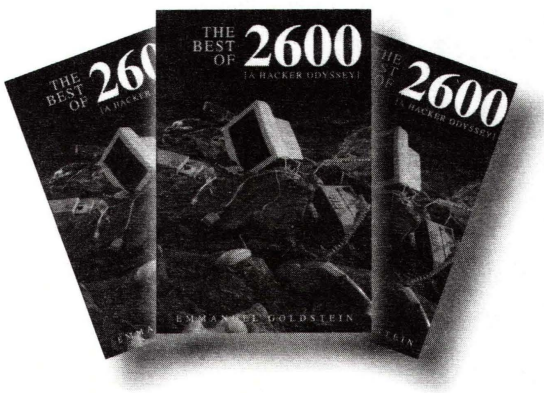
```
Jan 15 00:33:54 mythbox IN=eth0 OUT=
MAC=00:14:bf:5b:2d:5c:00:13:d4:
➥ 78:18:c6:08:00 SRC=12.24.36.48
DST=192.168.1.27 LEN=44 TOS=0x00
➥ PREC=0x00 TTL=43
➥ ID=16809 PROTO=TCP
SPT=63815 DPT=234 WINDOW=4096
➥ RES=0x00 SYN URGP=0
Jan 155 00:33:54 mythbox
➥ IN=eth0 OUT=
MAC=00:14:bf:5b:2d:5c:00:13:d4
➥:78:18:c6:08:00 SRC=3.6.9.12
DST=192.168.1.27 LEN=44 TOS=0x00
➥ PREC=0x00 TTL=42
➥ ID=16809 PROTO=TCP
SPT=63815 DPT=234 WINDOW=3072
➥ RES=0x00 SYN URGP=0
Jan 15 00:33:54 mythbox IN=eth0 OUT=
MAC=00:14:bf:5b:2d:5c:00:13:d4:7
➥8:18:c6:08:00 SRC=5.25.125.250
DST=192.168.1.27 LEN=44 TOS=0x00
➥ PREC=0x00 TTL=42
➥ ID=16809 PROTO=TCP
SPT=63815 DPT=234 WINDOW=3072
➥ RES=0x00 SYN URGP=0
```

Well, well, well. Just like the manual said, the firewall logs show that access was attempted from our specified address above, in the exact order that we inputted them. You can discover this for yourself by looking at the log messages and noticing what SRC equals.

So let's recap what we have (hopefully) learned today. We learned how to change your IP address while scanning, and that you can use an array of IP address to pretend to be other IPs while scanning. So you might be wondering at this point why I say we *almost* hid our identity. Well, if you have been paying attention to the firewall logs you might have noticed that the attacking MAC address has stayed the same. Of course, this can be changed as well, but that is another article for another time.

Resources

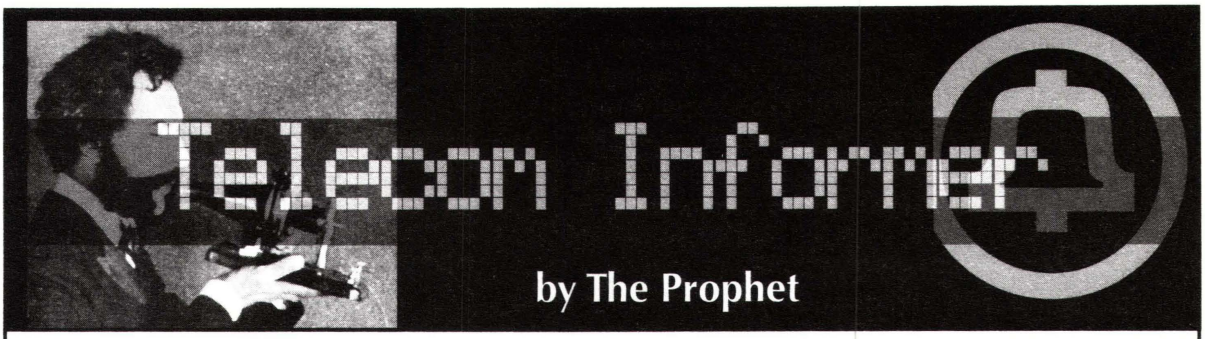
1. Nmap website: `http://www.➥insecure.org/nmap/`
2. Performance: `http://www.insecure.➥org/nmap/man/man-performance.➥html`
3. Port Scanning Basics: `http://www.➥insecure.org/nmap/man/man-➥port-scanning-basics.html`
4. Address Spoofing: `http://www.➥insecure.org/nmap/man/man-➥bypass-firewalls-ids.html`



The Best of 2600: A Hacker Odyssey

The 600-page hardcover collection can be found at bookstores everywhere and at http://amazon.com/2600

The special "collector's edition" is also available in rapidly dwindling numbers.



Hello, and greetings from the Central Office! It's autumn in Puget Sound country, which means the skies have returned to their usual leaden gray. It also means leaves from my no-good, lazy unemployed neighbor's trees are covering my lawn. After all, he's too busy cashing unemployment checks and watching *Jerry Springer* to do any actual work. I'm thinking of returning this week's batch of leaves in his mailbox, special delivery, with a few extra copies of his overdue phone bill and maybe a rotting salmon carcass for good measure.

All this fuming got me to thinking what would happen if my deadbeat neighbor's line is disconnected for nonpayment. He'll probably be reduced to calling his parents collect to beg them for money. I'm not a big fan of my neighbor, but I like his parents, and I'd hate for them to be stuck with a whopper of a bill. Although 97 percent of collect calls are from prisons and jails, there are still a healthy number of collect calls in the mix. And as it turns out, unlike in the good old days of the Bell System where rates were high but at least consistent, today's collect calling rates range from high to completely outrageous.

Younger readers growing up in the world of unlimited cell phone plans and unlimited long distance may not even know what a collect call is, or how to use other types of operator handled calls. In a world where long distance calling is effectively free, it's very unusual for many types of operator handled calls to be made these days. However, the following operator handled call types are still available from AT&T long distance operators and from local ILEC phone company operators (although you may have trouble finding an operator who actually knows how to place them).

All billing for operator-handled calls is either based on a station-to-station or person-to-person call:

Station to Station: This is the same billing as just dialing 1+ (NPA) NXX-XXXX direct, but you can have an operator dial the call for you. Operator dialed station-to-station calls are generally handled for visually impaired or disabled customers, and extra charges are waived for such customers. In general, operators only dial station-to-station calls for ordinary customers when they report trouble on the line, and surcharges are also waived in such instances. However, station-to-station rates can also apply to calls with special billing arrangements or where "time and charges" is requested.

Person to Person: When long distance calls were very expensive (particularly international long distance calls), you took a big financial risk by calling station-to-station. If the person you were trying to reach wasn't there, but someone else answered the phone, you'd still have to pay for the call. With a person-to-person call, the operator takes the name of the person you are attempting to reach and will try to contact that person directly. You are only connected (and charged for the call) if the operator can reach your party. Of course, a hefty surcharge is collected for this service.

Once you decide the type of call you want to make (assumed to be station-to-station if you don't specify otherwise), you must decide how to pay:

Calling Number: You can bill the phone number from which you're calling - provided it's not blocked. This billing method is often used by PBX and VMB phreaks. Believe it or not, some COCOTS allow this too!

Calling Card: The ILECs and many independent phone companies issue calling cards. These can be used all over the world to charge calls to your home telephone bill - generally at outrageous rates. These are different than calling cards issued by long distance carriers, for which calls are billed directly rather than being billed through your telephone company. Note that long distance carriers can bill ILEC calling cards, but it doesn't work the other way around.

Collect: When you make a collect call, it's free to you. However, the person you are calling must agree to pay the charges. Overseas, this is called a "reverse charge" call. Speaking of calling overseas, it's possible to call phone numbers in the U.S. collect using the dominant fixed line carrier (such as NTT in Japan, BT in the UK, Telkom in South Africa, etc.) and vice-versa.

Third Number: You can bill someone else's phone number for a call you want to make. In fact, you can call anywhere in the world - as long as they agree to pay the charges. You wouldn't believe how often people will agree

to pay for your calls!

Time and Charges: You can request that a call be placed with "time and charges." The operator will place the call with the type and billing you direct. After the call is completed, an operator will come back on the line to say how long you talked and how much the call cost.

Busy Line Interrupt: If you claim there is an emergency and agree to pay a fee for the service, an operator can break in and interrupt a call in progress. The operator will not connect your call to the existing call in progress, but will inform the called party that you are trying to reach them.

Busy Line Verification: An operator can verify that a line that rings busy is actually busy (not just off hook).

It's worth noting that CLEC, independent, mobile phone, and competitive long distance carriers are not generally required to offer operator services, except to the disabled. Where they do so, available services may vary. It can be fun finding out which services are offered, and how accurate the billing is.

But I digress. Back to my pitiful neighbor and the collect call he'll be making to his parents. The traditional way to call collect (from either a fortress phone or a POTS line) is to dial 0 plus the area code and phone number you're calling. You'll hear a "bong" tone, at which time you dial 0. Either an operator or (as is usually the case these days) an automated operator will ask you what type of call you are making: collect, billed to a third number, or billed to a calling card. If you're calling collect or billing a third number, a Line Information Database (LIDB) lookup is processed on the back end to determine whether the number you are calling is authorized for billing. In general, only fixed-line residential and business numbers can be billed for such calls, and most CLECs and VoIP providers do not support this billing type. Assuming that this criteria is met (and believe me, given the number of disconnect orders I'm processing on a daily basis, it's a rapidly dwindling criteria), you'll be asked for your name. Otherwise, you'll be asked to pay another way.

The operator will then dial the number you are billing and will ask if the charges are authorized. If someone at that number accepts the charges, your call will be connected. If it's a collect call, you'll be connected to the number you're billing. If it's a third-party billed call, you'll be connected to the number you're calling.

Third-party billed calls are not always verified before they are connected. This is at the discretion of the carrier and generally depends upon the type of phone you're calling from. For example, if you're calling from a home telephone or business line, AT&T will third-party bill calls without verification provided that a LIDB lookup indicates the line can be billed (or the LIDB lookup fails, which happens occasionally). If charges are disputed by the third party, AT&T will back-charge the originating number. However, if the charges are again disputed, AT&T simply eats the loss and blacklists the originating number for future unverified third-party billed calls.

When you follow the standard procedure to place a "0+" call, you will more likely than not be connected to an "alternative operator service" or AOS. OCI was one of the first carriers in this market, charging very high rates to consumers and paying fat commissions to owners of payphones choosing their services. Their operator service platform was poorly designed and their operators were poorly trained, so OCI was frequently exploited by phreaks in the early 1990s. Even today, shady AOS practices continue; consumer complaints are rampant about charges exceeding $5 per minute for collect calls. Muddying the picture further are toll-free "dial-around" services such as 1-800-FAIRCALL and 1-800-COLLECT, which are completely unregulated. Here are some example rates for a collect call:

- **1-800-ONE-DIME:** Operated by Sprint; 10 cents per minute plus a $2.99 operator surcharge.
- **1-800-COLLECT:** Operated by Verizon; $4.99-$6.49 surcharge, 55 cent additional payphone surcharge, $1.59 per minute + 12.9 percent USF plus tax.
- **1-800-CALL-ATT:** This service allows collect calls to prepaid and post-paid cell phones from AT&T, Sprint, and T-Mobile post-paid accounts. The charge is a flat $9.99 for up to 20 minutes. If you're calling a landline using 1-800-CALL-ATT, it's paradoxically more expensive: there is a $7.50 surcharge and the rate is $1.29 per minute plus 12.9% percent plus tax.
- **1-800-CALL4LES(S):** $3.99 surcharge, 25 cents per minute flat, allows billing to cell phones (excluding Verizon and Alltel).
- **Qwest 0+:** For intraLATA calls in Washington State, 50 cents to connect and 45 cents per minute.

The ability to call cellular phones collect is a relatively new development. To accomplish this, carriers use the premium SMS platform for billing (I have written about this topic previously).

Well, I'm out of space in this column, so it's time to rake my lawn again and bring this issue of "The Telecom Informer" to a close. I'll see you again in the winter. In the meantime, keep our operators busy making person-to-person third party billed calls with time and charges!

Hello!

Google Calling

by Faz and caphrim007

GrandCentral, now known as Google Voice (`http://www.google.com/voice`) is, like all Google services, a beta offering that was available through invitation only, though it appears the service will become more public in the near future. With Google Voice, you can choose a phone number and then link all of your phones to this main number to help maintain your privacy (by not giving out your personal phone numbers) and to promote a 'follow my phone' type offering. By linking your phone numbers to the selected Google Voice phone number, anyone calling your Google Voice number will automatically ring all of your linked phones. You can link your home phone, cell phone, pay-as-you-go phone, work phone, girlfriend's phone, and pizza parlor ("Hello, Mario's Pizza. Faz? There is no Faz here.") to your Google Voice number via the web interface. You can also initiate dialing from one of your linked phones in the Voice web interface to another phone number, and your Google Voice phone number will show up in the CallerID, even though you may be talking from your cell phone.

Now comes the fun part. There is no validation of the phone numbers you link to your Google Voice number! That is, you simply input the phone numbers you wish to be rung when a call comes into your Google Voice number. That's it. Nothing more. For outgoing dialing, you select the phone from your list, then input a number to call. This action then rings your selected number, then rings the remote number and connects the two. There are many opportunities here for those wishing to enhance voice communication offerings, to make free calls, or to simply have fun:

1. Link all your state representatives' phone numbers (be sure to include personal and cell if you have them!) to a single Google Voice number and publish to the web. Anyone who calls the Google Voice number will automatically ring all the representatives' phones.
2. Link a pizza place, then place a call through Google Voice to another pizza place. "Hello, Domino's. Huh? This is Pizza Hut, why are you calling me? I didn't, you called me. No I didn't."
3. Make free calls from pay phones. It is trivial to obtain phone numbers from payphones (if you don't know how, review past issues of *2600*). Link these numbers to your Google Voice number and initiate a call between them *for free*. This is great for covert meet ups.
4. Initiate a call between an evil hacker and the FBI.
5. Many Apple Stores have iPhones on display and active for calls by anyone who walks up. Get the phone numbers, link them in your Google Voice number then publish it to the web as free Microsoft Support. As an added bonus, initiate a call between the linked iPhones and Verizon tech support!

The drawback to the above is that you cannot listen in on the fun. However, if you have two Google Voice accounts, you can the abuse the on-the-fly conference feature. Simply establish a call between one of your phones and an external party (Pizza Hut), and, at the same time and using a different account, establish a call from another external party (Domino's) to your Google Voice number and conference them in while they are ringing. You now have a 3-way conference call!

The list of potential (mis)use* is endless. Thanks Google!

*One way that Google may be able to stop this, or at least limit the scope of misuse, is to immediately ring the phone numbers that you add to your Google Voice number and prompt you to input a security code. This will force you to be present at the phones you list. But, as of this writing, this is not required.

by J. P. Armstrong
jp@hackmiami.org

December 21, 2012 is just around the corner. A supposed cataclysmic event is to happen that day. Could doomsday be triggered by a shift in the magnetic poles, or perhaps some unstoppable airborne virus? Who knows! Either way you have to ask yourself, "Am I ready?" If the apocalypse happens in 2012 you don't want to be caught with your pants down. You'll need to be prepared. First things first, watch all the apocalyptic and zombie movies ever made. Including the foreign ones! You don't want to be one of the few humans left not knowing what to do.

You've watched the movies and now you must prepare for the worst. You're going to need a bunker deep inside a mountain, preferably at high elevation–if it's not magnetic poles shifting it will be global warming that takes us out. You will need some form of communication. That pwned iPhone just won't do. Sure it's unlocked for use on any service provider, but on doomsday, it's more than likely that you won't be getting any reception. That's why it's good to have an amateur radio! Many ham radios act like scanners. So you can listen to different frequencies like airband, police, fire & rescue, CB, GMRS, FRS, shortwave, AM, FM, amateur bands and your local Mickie D's drive-thru. Look for "wide receive" feature.

To prepare to communicate after doomsday, you're going to need to practice, and for that you'll need to get an amateur radio license. In the US, there are three types of license classes: Technician, General, and Extra. A Technician class license is the first one you get and has the most restrictions on amateur bands. Extra class licenses have the least restrictions. They no longer test for Morse code.Take one, two, or all three exams for only $14. Go to `http://arrl.org/`to see when they are having exams in your area.

Many local amateur radio clubs in the US have an annual Field Day. It's usually the last weekend of June. Field Days gives hams an opportunity to go outside and test out their emergency radio equipment. Just imagine thousands of people across the country setting up a makeshift communications infrastructure to prepare themselves for an actual emergency. Many times, it's amateur radio operators who are first to get on the air to coordinate relief efforts. Look up ARES or RACES for more info.

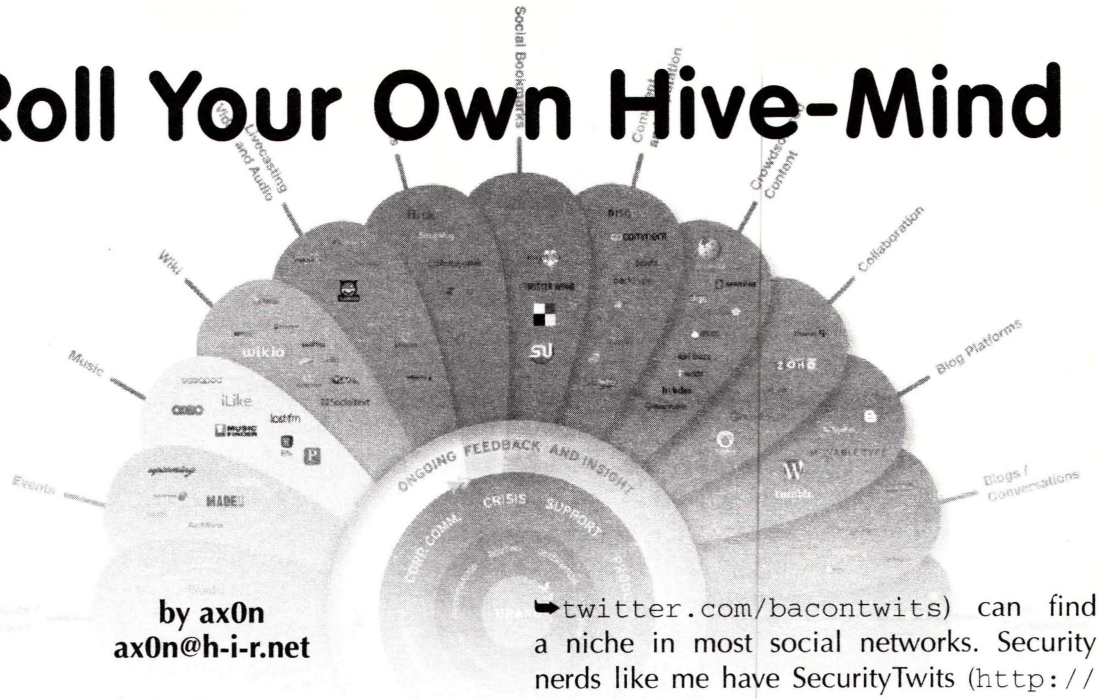
Getting a scanner may not be good enough. Consider getting a software-defined radio. It's a type of radio that can be connected to your computer via USB. With the help of GNU Radio, you can write custom code to do spectrum analyzing, modulation/demodulation, filters, HDTV tuning, and packet sniffing. Maybe after doomsday, the Internet will be severely crippled. Transatlantic telecommunication cables may very well be destroyed. Once human tribes have been established, you and other radio operators can set up bulletin board system (BBS) style nets with the help of software-defined radios.

It's more than likely that doomsday is not December 21, 2012, but if it is, and you have a ham radio, consider yourself covered (at least on the communications side). For the rest of the survival guide, I suggest watching those movies.

For more info on amateur radio check out: `http://hackmiami.org/wiki/Ham_➥Radio`.

Shout-outs: Ed, BSoDTV, and the HACKMIAMI crew!

Roll Your Own Hive-Mind



by ax0n
ax0n@h-i-r.net

There's no doubt that social networking is all the rage on the Internet these days. Places like MySpace and Facebook have become ubiquitous social hubs that start out as a circle of your real-life friends. Eventually, others join in that you've probably never met and might never meet in your lifetime. Your reasons for befriending them may be many: interesting photos or content, similar interests, or simply because they're a friend of a friend (of a friend of a friend). Maybe, you just like to compete in the popularity contest to see how many e-friends you can collect.

LinkedIn has a business focus. Maybe that's where you keep all of your professional contacts or hunt for job opportunities. Brightkite is a location-aware microblog with photo hosting ability; like Twitter on steroids. Maybe that's how you find out who hangs out at your favorite local places when you're looking for new friends. Friendfeed can aggregate most content from your other social network accounts. Maybe that's where you go to get your 50,000 foot view of your online social sphere.

What if you wanted to craft a specialized hive-mind, though? I'm interested in security, and I've found that, online, quite a few security geeks have blogs, Twitter accounts, Facebook profiles, and the like.

Instead of just looking for your existing friends online, you can leverage microblogging services like Twitter to find and follow like-minded strangers. Obviously, self-described social media addicts have no problem finding their cliques, but everyone from World of Warcraft Gamers (`http://twitter.com/WoWInsider`) to Bacon-lovers (`http://twitter.com/bacontwits`) can find a niche in most social networks. Security nerds like me have SecurityTwits (`http://twitter.com/securitytwits`).

The people you follow will frequently ask or answer questions of other folks. You can follow them as well, and pretty soon you end up with a news-feed of data you're interested in. Assuming enough of them follow you back, you will have a powerful hive-mind at your fingertips. This collective will give input on ideas from within itself. It will refine, disprove, or validate answers given to questions within the collective. It will link to fascinating content elsewhere on the web that other members might not otherwise find. It will challenge you to participate by giving as much as you get.

I've found that this hive-mind functionality works best on lightweight services like the aforementioned Twitter, or with link-sharing tools like Delicious, Digg, and Google Reader. Facebook and MySpace are far too cumbersome and broad-sweeping in their content to be used efficiently. Plus, most of the services I mentioned have easy-to-use RSS feeds that can be indexed, processed, aggregated, and searched later.

Of course, if you want people in your niche to acknowledge your existence on these social networks, you need to establish your presence with relevant content that's equally as interesting to them as their content is to you. Jumping onto Twitter and following every single member of SecurityTwits, for example, won't immediately integrate you into the hive. By lurking, however, you can learn a lot.

Free DirecTV on

by Outlawyr

First, the usual disclaimer: Don't do the crime if you can't do the time. Don't do it!

And now, on to the show.

I recently flew on Frontier Airlines for the first time. Not bad for a discount airline. They must not whip their employees like the other carriers. The airline is in Chapter 11, but has actually started turning a profit as of November 2008, so perhaps that accounts for the cheerful disposition.

Anyway, every seat has its own little TV screen with DirecTV, a broadcast satellite service controlled by Liberty Media. On your arm rest you have controls for volume, channel and brightness, as well as a standard stereo headphone jack. If you turn brightness all the way down, the screen goes black. Earplugs are free, but after the initial teaser phase when you can channel surf at will, a message comes up telling you to stick your credit card in the slot if you want to continue watching. Satellite TV is $5.99. Movies are $8, and there are 3 to choose from. Frugal man that I am, I resisted the urge to give up my hard earned money for a couple hours of television. But this left me time to ponder how one might hack the system and watch for free.

At first, I tried playing with various button combinations, but this got me nowhere. Then I remembered that I'd been carrying around an old American Express gift card. These cards look and function like a credit card, but have a predetermined amount on them when purchased. The one I had was originally worth $100, but I'd used it all, so the balance was $0. Unlike a credit card, this gift card isn't traceable to an individual. Of course, they know who is sitting in what seat on the airplane, but one can always play dumb. How was I to know what the balance was on the card? And, this was all in the name of science. If it wasn't for science, we wouldn't even have airplanes. Or DirecTV. Or gift cards. Thanks science!

So I swiped my gift card in the credit card slot, figuring that they don't process the credit cards while in flight, but rather wait until thvey land. After all, why clog the airways with more transmissions? After swiping the card I was told to press the up channel button to confirm, and then, like magic, I had access to all channels, including the 3 movies. I then turned the brightness all the way down, because there really was nothing interesting on. Solving this little puzzle did, however, serve my purpose of killing some time while stuck in a tiny little seat.

This, of course, leads one to ponder what other situations require a credit card but don't actually run the card at the time of purchase. Since I always carry my zero value gift card with me, I'm sure I'll get a chance to test it out in the future (without breaking any laws of course). If anyone has some insight, I'd love to hear from you.

Resources

- American Express gift card `http://www.americanexpress.com/gift/giftcardslanding.shtml`
- Frontier Airlines `http://www.frontierairlines.com/frontier/home.do`

Shoutout to my lady, Mrs. Outlawyr!

by hostileapostle

First of all, as a disclaimer, the following information is intended for informational purposes only. While this information is already widely available to anyone who wishes to find it, please follow the golden rule and don't do anything you wouldn't want done to you.

I get really frustrated sometimes when a website advertises a limited "free trial" and then asks for my credit card information. There is no good reason for them to have my credit card number if the free trial is really free. Of course, their plan is to start billing you if you don't cancel within the trial period. However, my opinion is that this is bad business practice, and I'm happy to circumvent it if I can.

Fortunately, some, if not most, of these web sites will not check to see if the number is real. They will only check to see if it is valid. Many of the readers here probably know that credit card numbers are generated using something a "Luhn check." A Luhn check is a very simple algorithm which doubles the odd digits and does a sum to see if the number is divisible by 10. The credit card companies actually use a slightly modified version of this algorithm that involves a check digit. This is the very last digit of the credit card number. With that said, here are the steps to produce a number that will pass the Luhn check on a 16-digit card number:

1. Starting with the first digit, double every other number.
2. If doubling a number results in a two-digit number, add those digits together to produce a single-digit number.
3. Replace the odd digits with the new ones just created. You should now have 16 numbers consisting. of the new numbers and the original even numbers.
4. Add up all sixteen numbers.
5. Manipulate the check digit so that the sum is divisible by 10.

So, as an example, let's use a random number, say 4264 1658 2275 1393. After doubling the odd digits and summing the ones that end up being two digits, we get 8234 2618 4255 2393. The sum of these digits is 67, which is not divisible by 10. So, to fix this, we change the check digit from 3 to 6. Our valid number is now 4264 1658 2275 1396. Whether that is really somebody's card number is anyone's guess.

One other thing I did here was I made sure the first digit was 4. This identifies the number as a Visa number. I don't know how picky the different websites are, but it's easy enough to include this digit. Here are the numbers for the major credit card companies:

3 - American Express
4 - Visa
5 - MasterCard
6 - Discover

I used this method a while back to obtain a free trial from `http://www.realtytrac.➥com/`. Of course, there's the small chance I could have just gotten lucky and found someone's real number, so I cancelled before the trial period ended, just in case.

It would be a no-brainer to write a script to spit out millions of valid numbers, but if you need that many, I fear what you might be doing with them. Hope this helps you get some free trials.

If You Can't Stand the Heat, Hack the Computers!

Understanding OAS Heat Computers

Part Two

by The Philosopher

Programming the System

The next option in the menu of commands is perhaps the most exciting, as it increases the potential to learn about the system by way of practical application. Pressing 'P' at the prompt will result in the following sub-prompt for a password:

```
PASSWORD:
```

If an invalid password is entered twice, the OAS will output the directive, "redial" to the screen, spew a line of garbage text, and disconnect the user:

```
PASSWORD: INVALID
REDIAL
4_QKvhb hC\v5(ij%Tud y% !#`&X
➥WJd,U 'MOu@,D+-LS
NO CARRIER
```

Defaults for this are unknown, although it is likely that they exist and are given to customers at the brief seminar that is recommended for all new OAS owners to attend. If one is truly determined to know the password, I would recommend that the interested hacker also visit the seminar. No features that log invalid password attempts are documented. Passwords do not echo to the terminal. The programming option is used to set every consequential element of the system from time set points to hardware handling. Passwords are ten characters in maximum length, an attribute revealed by the audible bell (Control-G character) heard when an eleventh character is entered–this bell will also sound at the MODE: prompt when input in excess of the expected is entered. When a correct password is entered a main menu of four options will appear. The four main options are as follows:

```
1.      CLOCK, DATE
2.      SET POINTS
3.      MISCELLANEOUS
4.      DIALOUT
```

Selection of any one of these will open a sub-menu of options followed by a question mark. For example, the following options may be displayed in the "MISCELLANEOUS" sub-menu 3:

```
OVERIDE/NORMAL?
SENSORS?
SENSOR LABELS?
METERS?
METER LABELS?
STEAM/HYDRONIC?
BURNER SIGNAL?
VERSION NOTES?
PASSWORD?
```

In order to program any of the options in any sub-menu, input the desired value followed by a carriage return <CR>. If a <CR> is pressed without an alteration in value the next option in the submenu will be displayed. To navigate through the sub-menus without programming, simply press ENTER at the option prompts. As is the case with the main 'MODE:' menu, typing a question mark will display all of the potential values for a programmable option, ESC is used to exit from programming mode altogether (upon which a password need not be supplied to reenter during the session), and BACKSPACE cancels an entire line of input. If an invalid value is entered, "INVALID ?=HELP" will be printed.

Sub-menu Notes

Sub-menus 1,2, and 4 are straightforward–programming of the clock, date, set points as seen in the 'S' mode, and dialout numbers/alarm conditions is accomplished here. The "MISCELLANEOUS" sub-menu, however, requires some explanation. The first option, OVERIDE/NORMAL, will set the system in a heat call for one hour if the override value is entered–it may be interrupted at any time during the cycle and turned off, returning the system to 'normal' operation. At "SENSORS?" one may manipulate privileges of the apartment temperature sensors (priority) and turn the outside temperature and aquastat sensors on and off. Sensor and meter labels refer to the headings that denote the thermistors and water meter in the current report "R." 'METERS?" provides the options to turn the water meters on and off, combine the pulse inputs to a single, double-headed meter, specify a scale factor for the flow rate, and to turn the water records on and off. "STEAM/HYDRONIC?" is only useful on the single model of heat computers that may be used for steam or hydronic systems, controlling reporting options. "BURNER SIGNAL?" does not control the burner control signal, which activates the burner–it only permits the user to switch the monitoring of burner on and malfunction signals on or off. One may write "VERSION NOTES" in with the second-to-last

option; these will be seen with the "V" command and typically pertain to any idiosyncrasies of the boiler to which the computer is attached. The final option in this sub-menu enables the user to change the programming password, an action not advisable as the legitimate operator of the unit will undoubtedly notice the presence of an intruder upon discovering that the password last used is no longer valid; still, little recourse exists for this. Interestingly, it seems as if the password storage capability for certain models is more extensive than a single programming password, as some oil companies have been known to possess passwords in addition to building managers.

Controlling the Heat

For reasons of sheer practicality and to remain true to the title, here is a quick step-by-step tutorial regarding the actual setting of heat. At the "MODE:" menu, press "P" to enter programming mode and enter the password. Select sub-menu 2, set points, and navigate to the option to set the maximum temperatures under "day," "evening," and "night." Note the current definitions of all three times of day and select the appropriate point. To increase the heat, increase the maximum temperature permitted value as described above; to decrease heat, decrease this value. Alternately, one could input a manual override at the miscellaneous sub-menu to actuate a one hour heat call.

Other Modes

A few of the following modes are mere alternate manifestations or continuations of the data displayed in the report and are explained satisfactorily by the help command. T1, T2, and T3 are indeed nothing more than hourly temperature records in the following format, edited here for brevity:

```
MODE: T1
__TIME_245A_245B_245C_245D_285A_285B_285C_285D____9___10__OUT__AQS__DHW
➥_CHW_STK
12:00M 77 83 82 81 80 74 82 83 <5* <5*! 68 189 116 >>> 120
11:00P 76 82 82 80 81 76 82 83 <5* <5*! 69 181 116 >>> 120
10:00P 75 82 82 80 81 76 82 83 <5* <5*! 68 194 119 >>> 272
 9:00P 75 82 82 78 81 76 81 83 <5* <5*! 68 189 117 >>> 128
 8:00P 76 79 82 78 82 76 81 83 <5* <5*! 70 181 116 >>> 120
 7:00P 76 82 82 81 81 76 82 83 <5* <5*! 71 198 119 >>> 152
 6:00P 77 81 81 80 81 75 81 83 <5* <5*! 69 184 117 >>> 120
 5:00P 77 81 81 80 81 73 81 82 <5* <5*! 70 191 117 >>> 128
 4:00P 77 80 81 80 81 73 81 81 <5* <5*! 70 197 119 >>> 144
 3:00P 77 80 81 79 80 74 80 81 <5* <5*! 70 188 116 >>> 116
 2:00P 77 80 80 78 80 74 80 81 <5* <5*! 66 194 119 >>> 128
 1:00P 76 79 80 78 79 74 80 80 <5* <5*! 63 186 118 >>> 124
12:00N 76 79 80 78 79 75 80 80 <5* <5*! 66 180 119 >>> 120
```

The only moderately important distinctions here are the facts that "12:00M" and "12:00N" represent midnight and noon respectively, and that these tables conclude with 11:00 p.m. T2 and T3 are identical, differing only in the 24-hour days that they contain data for–T3 contains three-day-old information, etc. Similarly, "H" will provide the daily history of the data in the next lines of the report. This should appear familiar:

```
MODE: H
_DATE_BURNER__HEAT___BYP___MAL___BAT__HI__LO_
Jun 23   0:45   0:00   0:00   0:00   0:00   73   62
Jun 22   0:46   0:00   0:00   0:00   0:00   73   61
Jun 21   0:42   0:00   0:00   0:00   0:00   80   60
Jun 20   0:46   0:00   0:00   0:00   0:00   79   61
Jun 19   0:49   0:00   0:00   0:00   0:00   78   57
Jun 18   0:50   0:00   0:00   0:00   0:00   69   56
Jun 17   0:48   0:00   0:00   0:00   0:00   76   63
Jun 16   0:49   0:00   0:00   0:00   0:00   78   61
Jun 15   0:45   0:00   0:00   0:00   0:00   75   65
Jun 14   0:38   0:00   0:00   0:00   0:00 >90   69
Jun 13   0:46   0:00   0:00   0:00   0:00   89   74
Jun 12   0:46   0:00   0:00   0:00   0:00 >90   76
Jun 11   0:48   0:00   0:00   0:00   0:00 >90   75
Jun 10   0:51   0:00   0:00   0:00   0:00 >90   73

_DATE___H-A__H-W__L-W__H-S_____WTR_
Jun 23   198   127   106   664       0
Jun 22   200   125   109   668       4
Jun 21   200   125   107   668       0
etc...
```

This unit displayed this for every date up to June 10. XD 1-3, or "more hourly records" were not seen on this system at all and are probably boiler-specific, perhaps containing records such as the supply and return temperature that are only required on hydronic systems. Since some of the systems that one may hack might control hydronic boilers, it is important to retain a knowledge of their workings, information universal to all types of heat computers that manage such boilers. Recall the operation of hydronic boilers, specifically the process of water circulation. Quite simply, supply temperature refers to the temperature of water as it exits the boiler to circulate around the space that it is heating, and return temperature to that of the water as it returns to the boiler. Water records were also absent from this log, strongly suggesting that this is a steam system. Events, accessed by the command, "E" are entirely separate from the initial report, although some events may be recorded there without the time of their occurrence:

```
MODE: E
  8:27P OFF      12:16P  ON DHW          11:56P  ON DHW   2:51P   OFF
  8:21P ON DHW   11:47A  OFF            11:00P  OFF      2:47P   ON DHW
  7:50P OFF      11:42A  ON DHW         10:55P  ON DHW   1:52P   OFF
  7:46P ON DHW   11:10A  OFF            10:05P  OFF      1:47P   ON DHW
  7:04P OFF      11:05A  ON DHW         10:00P  ON DHW   1:00P   OFF
  6:59P ON DHW   9:15A   OFF            9:20P   OFF      12:55P  ON DHW
  6:05P OFF      9:15A   HEAT OFF9:16P  ON DHW  12:04P  OFF
  6:01P ON DHW   8:20A   ON             8:09P   OFF      12:00N  ON DHW
  5:35P OFF      8:19A   HEAT CALL      8:04P   ON DHW   11:17A  OFF
  5:30P ON DHW   7:06A   OFF            7:22P   OFF      11:12A  ON DHW
  4:49P OFF      7:06A   HEAT OFF7:16P  ON DHW  9:56A   OFF
  4:44P ON DHW   5:31A   ON             6:38P   OFF      9:56A   HEAT OFF
  4:00P OFF      5:30A   HEAT CALL      6:33P   ON DHW   9:00A   ON
  3:56P ON DHW   4:34A   OFF            5:59P   OFF      8:59A   HEAT CALL
  2:54P OFF      4:29A   ON DHW         5:54P   ON DHW   7:50A   OFF
  2:49P ON DHW   3:04A   OFF            5:03P   OFF      7:50A   HEAT OFF
  2:15P OFF      2:59A   ON DHW         4:58P   ON DHW   5:31A   ON
  2:10P ON DHW   1:15A   OFF            4:18P   OFF      5:30A   HEAT CALL
  1:29P OFF      1:10A   ON DHW         4:13P   ON DHW   5:07A   OFF
  1:24P ON DHW   12:00M  OFF            3:23P   OFF      5:03A   ON DHW
 12:21P OFF      12:00M  -----          3:18P   ON DHW   3:39A   OFF
```

This is a record of every burner on/off cycle for the past 84 events. Only ordinary heat and domestic hot water calls are seen above, but flame failures, overrides, bypasses and power failures may also be logged here depending upon the version.

As is evident by the redundancy present in several of the options, the entire system is designed to facilitate great discretion in what one views during a particular session. The only practical reason for offering all of the records as individual segments is that of specificity in monitoring. If one wishes to view a complete list of all of the records for a particular day in the past three days at the entry of a single command, D1, D2, and D3 are available. To conclude descriptions of all commands, "L" will redisplay the message first seen in the banner immediately upon connection to the system and "V" for Version will print a message similar to the following, with the version, date installed/configured, type of system and number of sensors:

```
MODE: V
V 6310 - 10 NOV 1995
On/Off System
8 SENSOR UNITAT
```

This confirms the previous suggestion to the effect that this is a steam system, as steam systems are also known as ON/OFF or HI/LO fire boilers.

Footprinting the System - A Review/Additional Tips on Obtaining the Password

Several ways exist through which information pertaining to the system may be acquired, information potentially useful in the attainment of the password and in programming of the settings. Commands such as "Version", "Water Records" and "More Hourly Records" should reveal with ease the general specifications of the OAS. This information, coupled with the CNAM data of the dialup (backspoofing, anyone?), address, and dial-out phone numbers, will likely prove extremely useful in either social engineering to obtain the programming password or guessing it in order to further one's exploration of the heat computer. One aspiring to program the OAS could also potentially attempt the age-old callback ruse, phoning the legitimate operator at a number listed under 'Set points' (Mode S) and leaving a message with a voice-mail number with a greeting identifying it as belonging to 'Optimum Applied Systems, Incorporated', accompanied by a statement to the effect that "Your heat computer has reached its ___ year point, and as such we need to perform diagnostic tests on the system as a part of your warranty..." and so forth. Do note, however, that the dialup or IP might be particularly difficult to obtain as the actual operator of the

system would logically be the only individual in possession of such information, thus rendering impersonation of him or her absolutely useless. Creative ways to get the dialup may be devised, though, although the best method as of yet seems to be a simple matter of wardialing the exchange controlled by the company that owns the OAS (in the case of large corporations with inclusive PBXs) or dialing around the phone numbers of the building in which it is likely to be located (with small businesses). Wardialing metropolitan prefixes is also bound to turn up heat computers, possibly of the OAS brand. Although the version 6310 does not support this, other versions may permit simultaneous logins and command execution in a single 'session', enabling one to "eavesdrop" and/or interfere with the session of the legitimate user. The programming password is not echoed to terminal or screen; however, it is, remember, unnecessary to enter the programming menu once it has been entered at the initial prompt. Also, while it may contain special characters, it is doubtful that it will be greatly protected; the ten-character password is likely to be vulnerable to a dictionary attack of words containing ten characters or less, especially since no evidence or mention is made or available anywhere of logging failed attempts. As a side note, the author of this article has heard of a few rumors of use of the OAS and similar heat computers by landlords to deny tenants heat in an quasi-extortive context or misuse resulting in active heating of a building in the summer or when the temperature outside is otherwise high. Wherever advanced technology exists, there will be people who are either ignorant or abusive of it, unfortunately. Although such incidents are certainly rare, OAS skills would be infinitely useful in the face of their occurrence, proving once again that knowledge regarding any type of technology that controls one's life is always of use to nearly anyone with any motives. Remember, if you can't stand the heat, get out of the kitchen and into the OAS!

The Software - An Addition

All of the above is merely the beginning. While connecting to the OAS heat computer via a terminal client and manually entering all of the commands might be satisfactory for some, OAS also offers software to automate and enhance the process of heat computer maintenance (whether it is authorized or not). This is an incredibly useful enhancement to the pursuit of hacking OAS Heat Computers, as it reveals several aspects otherwise hidden, and it has several useful utilities intended clearly for administration. This software, available on the OAS website for all to download, at `http://www.oas-inc.com/`, is called 'Master95' and can be quite somewhat of a kludge just to install, as OAS doesn't seem particularly disposed toward the idea of amateur experimenters logging into heat computers and running commands. If the reader will forgive the sudden launch into linear, redundant expository style and the informal shift into the second person, the following will explain the installation process. It comes in a strange archive format unknown to the WinRAR archive software, called an "SFX CAB Archive" as a .exe file, "STUB.EXE". If you attempt to open/run it as you would any other .exe file, by double-clicking on the icon (it doesn't run in DOS mode), you will receive a window prompting you for a case-sensitive password of enormous maximum length. Ignore that for the moment and open the archive in the archive management software of your choice–the author personally recommends WinRAR. A list of 16 files should appear, beginning with 'data1.cab' and ending with "_INST32I.EX_." Extract and copy all of these files to the desktop or other location where the entire installation process will take place (the desktop is recommended for the sake of convenience). Run SETUP.EXE (it should be the eighth file in the list). Does that text in the background of the window with the copyright and version appear at all familiar?) and proceed through all of the prompts-agree to the license, etc. Instruct the software to place an icon for Master95 onto the desktop when prompted to do so. Upon reaching the end of the InstallShield Wizard (the application that guides you through the setup process), click "Finish" and run the software by double-clicking on the desktop icon. The full version of Master95 Master Dial Program Version 1.96 is now installed.

The author is not aware of any additional features that may lie behind that password prompt–it may be reasonably assumed that none exist since the software itself is clearly labeled as the "Full Version" when "About" is selected. The OAS website also declares that the software, while downloadable, must be registered over the phone before use, (presumably with the purpose of the confirmation of one's status as a customer) lending credence to the notion that OAS does not intend for the public to have unhindered access to Master95 and that the password protection is a feeble form of security. If so, this is simply another instance of security through obscurity, assuming that one will not attempt to open it with archive software, an absurd assumption as it clearly identifies itself as an archive under "properties," with passwords absent. In any case, all of these files in the archive may be freely copied, and the software should operate without any difficulty if all of them are located in the same directory,

the directory in which it is run.

At first glance, the Master95 software appears to merely be an alternate way to access heat computers and administer them using a GUI and menu system, but it does reveal a few interesting things. Of foremost interest to the reader may be the commands help file, which presents in a succinct format all the descriptions of the current report, event log, etc, although it completely lacks explanation useful to an outsider (unauthorized user; i.e., hacker) such as explanations of ultimate application to heat and descriptions of boiler operation, as it assumes that the software user will be trained in such matters. Observing the window, one will notice that, under the "direct dial" option when the option "building list" is selected, other OAS products controllable over modem are listed–a mildly interesting bit of information. Perhaps it would be lucrative to watch wardial logs for anything mentioning a "tank computer" or a "fire eye." The following banner demonstrates the general format and appearance of tank computers, which are used to monitor liquid inside of tanks, such as oil:

```
OAS Tank Gauge 145 ATLANTIC
STREET 4:30P Sat Dec 17, 1993
TANK CAPACITY: 5000 GALLONS
```

These connect at 8,N,1 as the heat computer text does not display properly when a heat computer is dialed and either option is selected. Tank computers are a subject for another article. Upon establishing a connection to a heat computer through the software, one may enter commands manually in the blue terminal window in which all output is viewed, or using the drop-down menu system, if one prefers a GUI. Notice the command "Real Time Display", under "Commands" sent by the keyboard shortcut Alt+R. Selection of this during a session will pull up a "Command Select" box, with four commands listed that accomplish this-R RA, RB, and XR. RA and RB will not work on this particular model/type of heat computer at all, and may produce erratic results on other models. XR, however, displays the report and alters it in real-time. This is a hidden command, not documented in the list provided with a "?"! While in most cases the two reports may be identical, a slight discrepancy may be seen between them, a display of the constantly fluctuating temperature of the area surrounding thermistors.

Master95 also serves as an effective organizational tool for heat computer management, incorporating into its array of utilities a building list in which heat computers (and the other types of systems) may be sorted based upon address, an assigned ID, and dialup. Editing the properties of a particular building in this list entails the assignment of an ID, setting the type of unit (Heat, Oil Tank, Heat 7000, or Fire Eye), the baud at which it connects, and the "port switch." Building lists may also be imported from older, DOS versions of Master software with the file option, "Import Old List." "Tools" for building lists include daily and single collection, summer/winter programming, and clock programming. The latter two are simply an automation of the programming set points process for the summer/winter option and time. The password box only accepts ten characters, revealing the aforementioned fact that passwords are ten characters long. Daily/single collection is a slightly more complex automation, in which the user may program the software to dial selected buildings in the list at a specified time and day, execute commands, and store the output in a file with the extension .sum, for "collection summary." To configure these parameters, select "Setup Parameters" under the "Tools" menu.

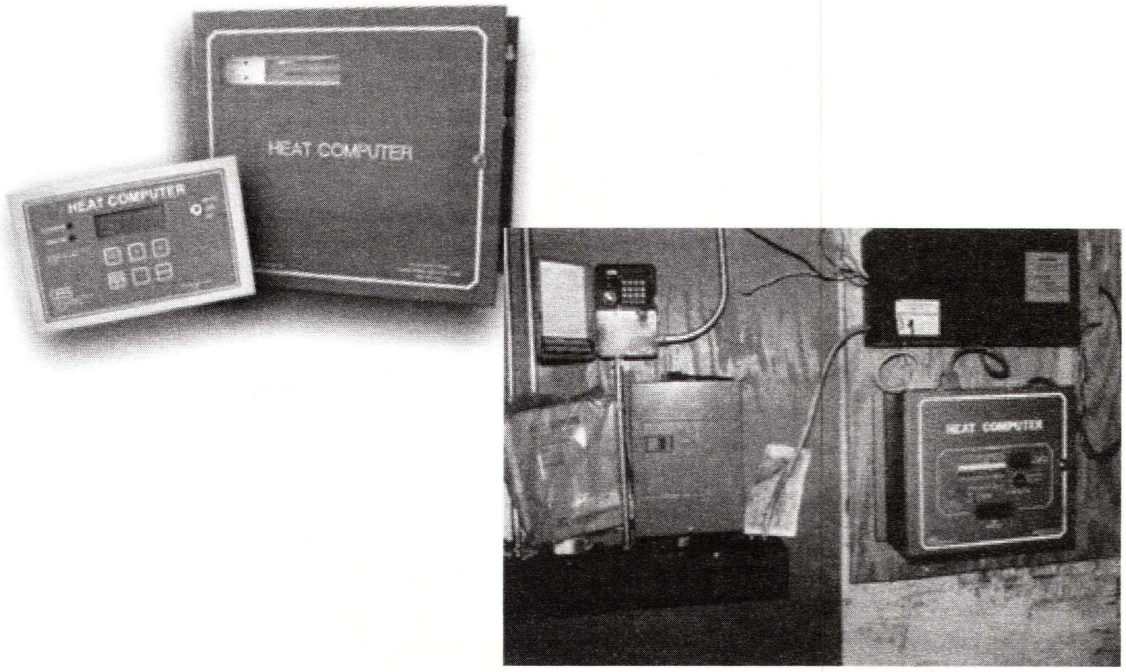
Conclusion-Thoughts on Security

While in some regards OAS can hardly be blamed for certain aspects of the nature of heat computers that render them so incredibly predisposed to control by outsiders–attributes such as the remote accessibility over phone lines, un-passworded execution of seemingly harmless commands, and so forth, leaving such systems that control heat to an entire building lying about on the PSTN and, recently, the Internet, is frankly unwise. OAS is extremely zealous in advertising, providing details as to the technical specifications of models sold in numerous public releases. The problem as here present insofar as security is primarily that a very limited amount of seemingly innocuous information can lead to extremely specific information useful in penetrating and taking complete control of specific units; for instance, the attainment of the dialup to a heat computer can lead to the address of the unit and possible numbers at which the owners/operators may be contacted. One could even carry this social engineering scheme so far as to call up the building owner/manager with an actual problem visible in the report, a difficulty only repairable by remote programming, and proceed to correct it upon learning the password! A simple understanding of human nature suggests that people will be much more susceptible to social engineering, that is, much more willing to give out the programming password, when faced with a potential disaster such as complete cutoff of heat in the dead of winter, or even something minor such as a small water leak or a dirty coil. And, while I most certainly do not condone exaggeration of the problem, all of this is definitely something to ponder as these systems begin to make their way onto the Internet. While manufacturers of some devices

have realized the folly of unnecessary remote access, heat and building automation systems are likely to become even more accessible in the future, for evident reasons of expediency. From an explorer's standpoint, heat computers of all types provide a relatively safe venue through which a fairly extensive assortment of technologies may be studied–boilers are nearly as complex and interesting as phone systems or any one of the other self-contained networks of mechanical and electronic parts that comprise the modern world. Still, the thought that an individual in a remote location could with relative ease (here it is important to remember that while OAS Heat Computers may be uncommon, other heat computers and building maintenance systems exist in abundance, especially in large cities) direct the equipment that administers heat and water to a large building is slightly disturbing. If, by any stroke of fortune, the curious hacker reading this article should happen to find an OAS Heat Computer, I advise him or her to align subsequent actions with the Hacker Ethic, to refrain from actuating the causation of any permanent or immediately serious problems with the system either unintentionally (as preposterous as that may sound) or intentionally, as a matter of course.

A grayscale photograph of an OAS Heat Computer unit is available at the time of this writing on `http://www.homeenergy.org/➥archive/hem.dis.anl.gov/eehem/➥picts/97054101.gif`, and other pictures of the front panel are available on `http://www.oas-inc.com/`.

Shoutouts to rev, whitehorse, ThoughtPhreaker, Substance, DCFlux, bomberman2525, radio_phreak, everyone in #telephony, Binrev and the DDP, the broad class of people who ever wrote anything that contributed to my underground knowledge base, the anonymous person who posted the logs that initially brought heat computers to my attention, and OAS for manufacturing such interesting, useful, and vulnerable products. If I have forgotten or omitted anyone else, please forgive me with the assurance that your contributions and the general benefits of our interactions do not go unnoticed and underemphasized. I may be contacted on IRC on 2600net in #2600, #telephreak, and #telephony, on the Telephreak BBS at `telnet://bbs.telephreak.org`, or at my email address: `philosopher2600@➥gmail.com` with any questions or input. If anyone should happen to possess a superior command of such systems as were discussed in this article, I would like to hear from you; to this end I encourage the use of the letters section of *2600* as a public forum to further knowledge upon this topic. Although it was extensively researched, I authored this article strictly from the perspective of an outside hacker experimenting with the system-a good deal of information presented here was garnered from experimentation and observation, and as such is not all-inclusive by any means, although conjecture and speculation is labeled as such. Redundancy here (presentation of details present in the help file of the Master95 software and so forth) exists in order to provide readers with a reference that may be used both as a quick guide to heat computers without the help file or the official manuals, as well as an explanation of, in the true spirit of hacking, potential unintended uses for the various options therein. Slight details are available in the help file of Master95 and elsewhere that are not mentioned here–get the software!



The Medium is the Mess-Up or: How to Hack the World

Most of us know and understand that the major power of today's world is the media. Whoever controls the media controls everything. And since the media is not nature but culture - Western culture - it is always owned by somebody. There's no such thing as free media. It's (as always) about controlling the means of production. So long as you can't download your iPhone, all our so-called free media, our Creative Commons tracks, freedom of speech and Twitter, it's all bullshit.

Media is the strongest political, economic, and, of course, heuristic power in the modern world. And most of us do not own significant parts of it. So if you want to do anything about it, you have to hack the system. That can be done with something called guerrilla communication. And I am about to tell you what that is and how it works, my black-shirt-with-penguin-wearing friends.

Guerrilla communication exists to fight the media system and the reality produced by this system. The word "guerrilla" suggests that there's a war going on. It also suggests that media defines and preserves the status quo. The status quo of a society in which knowledge and information are not only means of controlling people but also ways of segregating people into classes, like the working class and - that's us - the networking class.

So what can be done about it? The classic guerrilla communication tactic is to launch small but effective attacks on an enemy which is much bigger but also hampered due to institutionalization. These tactics are adapted from classical guerrilla warfare (which already made use of guerrilla communication against its enemy's communication system).

Unlike guerrilla warfare, guerrilla communications aim to interfere in the monologue of bourgeois mainstream media and to show how reality and normality are defined through media control and access to public spaces. It is inspired by various theorievs on social communication and includes positions that tend to focus merely on the government while excluding other factors from analysis, creating a simplified portrait of social powers. Some guerrilla communication theories may take left-wing or Marxist positions in regards to the social factors underlying and forming a society, such as class, race, or sex.

There's a wide range of strategies guerrilla communication could use. Most of them have something to do with mocking or mimicry of official communication.

I'm part of the political art/tech group monochrom. Some years ago we used these techniques to stage a deadly virus outbreak at "Art Basel Miami Beach," one of the biggest art fairs in North America. We wanted to address the hysteria of the post-September 11, 2001 attacks about biological warfare and the media coverage about bird flu. And we wanted to create a statement about the disgusting networking and business aspects of the art market. Our press release stated that Günther Friesinger (a member of our group) was carrying a "rare, but highly contaigent subform of the Arad-II Virus (Onoviridae family)." Günther was walking around the fair and did what every good businessman should do. Small talk, shake hands, spread business cards. But the business cards, of course, were "contagious" and a small group in hazmaz outfits later tried "to retrieve and destroy the business cards he has spread." Additionally, we told all the people that we had to take Günther into custody and would have to dissolve his body in acid. It was interesting to see how many people were thanking us for our service.

Mocking strategies are especially useful in attacking a single player like a multinational by trying to stain his image and tactically embarrass him as a warning to stop the evildoing. While this strategy is useful in pointing out the power of consumers, it still remains within the construct of "good" capitalism versus its evil twin "bad" capitalism. Never forget that there is no such thing as "good" or "bad" capitalism. Capitalism is a totalitarian doctrine whose very structure, purpose, and operating mode is considered to "alienate humans," to take control of and to modify their basic human needs and relationships.

Publicity means to expose yourself and therefore you can be attacked. Advertising is inherently public and something that tries to give instructions can be obeyed or disobeyed by not playing by the rules. You could, for example, decide to boycott a product as long as it is advertised. This could be a personal interpretation of guerrilla communication. One that sucks, I

guess, because it's rather naïve: it tends to be the best products which are advertised because they are advertised.

You could sabotage instructions by misinterpreting them and acting dumb. That goes for factory workers as well as for all you white collar supremacists: why not use the CD drive in your office computer as a coffee cup-holder? It's got a tinge of freedom to it which you, of course, wouldn't want to experience because it's dangerous. It's the freedom of something that exists beyond the mere functionality of the way it was intended. Oh wait - are you a hacker?

One of the basic strategies is faking things: press releases by political parties or companies, websites, even your own life. You could say that it's all about playing with representation and identity, alienation and identification. It means that you use affirmation to a degree that goes beyond the conventional to show what something really means - but also to act out the habits and conventions of your enemy. Guerrilla information, for example, mimics classical marketing tools and knowledge, but twists it in the opposite direction. This works for press releases and interviews, as well as for personal habits. The Yes Men, for example, are masters of the typical company spokesmen body language and tone of voice. What they do is no longer parody, but mimicry. You could say that guerrilla communication is not trying to destroy the dominant codes but rather to deconstruct and strategically abuse them for its own purposes.

It should be clear that guerrilla communication doesn't have a military goal in the classic sense of destruction, occupation, suppression, or extermination. It's about putting special groups like the people of Bhopal on the map of global consciousness.

One of our own exploits was started in 2001. My group monochrom was chosen to represent the Republic of Austria at the Sao Paulo Art Biennial in Sao Paulo, Brazil in 2002. However, the right-wing political climate in Austria (fuck, that was a bad time!) gave us concerns about acting as representatives of "our nation" (well, fuck our nation). But we decided to deal with the problem by creating the persona of Georg Paul Thomann, an irascible, controversial (and completely fictitious) artist of "longstanding fame and renown." Most of the work was writing his 500 page biography. The media reported about Thomann as the official Austrian representative - I guess they just didn't know how to google - and so our strange art avatar suddenly was a cultural ambassador of "our country." And all the members of monochrom were his technical support team. Through the implementation of this ironic mechanism - even the catalogue included the biography of the non-existent artist - we tried to hack the philosophical and bureaucratic dilemma attached to the system of representation. But moreover, Georg Paul Thomann proved to be a potent payload for political content. The artist Chien-Chi Chang was invited to the Biennial as the representative of Taiwan, but Taiwan's name tag was removed by people working for the administration. The country's name on his cube was replaced overnight by new adhesive letters: "Museum of Fine Arts, Taipei." For Chien-Chi Chang this was very irritating. His art piece dealt with the mistreatment of Taiwanese people in mental asylums, so it was very import for him to be the official Taiwanese representative. He tried to get information, but nobody wanted to inform him. We started some research and discovered that China had threatened to retreat from the Biennial - and create a bunch of diplomatic problems - if the organisers of the Biennial were thought to be challenging the "One-China policy." So we started a solidarity campaign and began to collect letters. A "t" from Austria (equals Aus ria). And the Canadians really didn't need all three "a's," etc., etc. And after some time Chang could remount a trashy new "Taiwan" outside his room. Chang was very pleased and several reporters took pictures and took notes. Several Asian newspapers reported on the performance. One Taiwanese newspaper headlined: "Austrian artist Georg Paul Thomann saves 'Taiwan.'"

A non-existing artist saves a country that shouldn't exist? Well, I love postmodernism.

You see, guerrilla communication is a versatile practice of cultural resistance. Information and political education are completely useless if nobody wants to listen. But this fact can be a powerful ally. Guerrilla communication doesn't focus on arguments and facts like traditional communication. Rather, it inhabits a militant political position; it is direct action in the space of social communication. But it doesn't aim to destroy the codes of power and signs of control. Communication guerrillas do not intend to occupy, interrupt, or destroy the dominant channels. They focus on detouring and subverting the messages transported.

What's new about all of this? Nothing. But standing on the shoulders of earlier avantgardes, the communication guerrilla doesn't claim the invention of a new politics or the foundation of a new movement. It is merely continuing an exploration of the jungle of interaction processes, senders, codes, and recipients.

The earliest forms of modern guerrilla communication can be found within the WWI art scene, when a group of international artists and deserters met in Zurich on neutral Swiss ground to launch the Dada movement, laying the foundations for such radical art movements as The Situationist International, Punk, and Neoism.

These people developed strategies to provoke and challenge society, to implement their political agenda into the public space, and to start reclaiming the streets. The street is synonymous for public space and the humdrum surface of society. Therefore, it was considered the perfect

stage for informing people or, rather, for counter-informing people. Most activists came from a classical art or journalist background but had reached the conclusion that nobody really listens when you speak in the traditional art space. Your average guy does not go to exhibitions or concerts and rarely sees counter culture media. Even if people would go, they would consider what happens there to be "just art." Art is the place where things might be reflected, but that amounts to nothing since it's removed from everyday life. Art is a special task and a special place for special people.

The post-bourgeois artists tried to bring art back to the people - not as a service (as it is to the bourgeois elite art consumer), but as a form of irritation. This was one of the many starting points of guerrilla communication as well as the so called "reclaim the streets" movement which includes funny yet irritating activities like Flash-mobs - and Adbusters.

In the 1970s, counterculture split into a more traditional Marxist wing consisting of small parties and groups that wasted a lot of their precious time and beautiful youth to fight each other. Plenty of their strategies, like throwing pies at celebrities, are still around in the guerrilla communication movement of today. They too started working with fake information and actions distributed via the bourgeois media, oblivious of the fact that it was spreading a hoax. A popular slogan suggested people "invent false facts in order to create real events," but they too made real objects and did cultural piracy stuff like pirate editions of the socialist classics or handing out counterfeit subway tickets. Pirate radio stations appeared and hijacked radio frequencies. Graffiti was an important weapon of that movement to overwrite the text of the city. In its best and most far-out moment, they came up with the post-modern idea that social structures are texts, too, and therefore can be overwritten in the same way you can overwrite an advertisement.

At the same time the squatters' movement emerged: Post-bourgeois artists attacking actual private property as well as non-material cultural property. Guerrilla communication - unlike everybody else - shows no respect for the fact that the media and the public space as well as the images and cultural frameworks we live in belong to the bourgeois. Its fundamental strategy is to misappropriate images, words, and radio frequencies and shift them to different contexts. In France, the Situationist Movement defined a form of art called "détournement." It means that you roam aimlessly around the streets and take what you find and then do something with it.

As part of monochrom, we promote a concept called "Sculpture Mobs." To quote our own pamphlet: "No one is safe from public sculptures, those endless atrocities! All of them labeled 'art in public space.' Unchallenging hunks of aesthetic metal in business parks, roundabouts, in shopping malls! It is time to create DIY public art! Get your hammers! Get your welding equipment!" So we started to host training sessions and we began teaching interested people how to erect public sculptures in under five minutes. Why under five minutes? Because that's the time you have if you set up a sculpture - let's say at a Wal-Mart parking lot - before "security arrives." As part of the project, we created a political illegal public sculpture called "The Great Firewall of China" at the Google Campus in Mountain View, California. And we set up various realistic looking antitank obstacles in inner districts of various cities. We named these pieces "New Kids On The Road Block."

So, in a certain way, guerrilla communication is hacking. And hacking is a means of guerrilla communication because it is a hostile assault from outside the system trying to find a way to change or manipulate it from within. You have to know how everything works - the way in which the media shapes and constitutes reality - just like hackers not only know what a website is and what it looks like and how it works, but also how the code - the very structure - works.

But what do we know about the cultural code of messages? Do we really understand how, for example, heterosexism is cemented in our society via texts and images? What about cultural stereotypes? How do we - or at least some of us - come to believe that white suburban males are meant to rule the world without even once spending a thought on it? How is the sexist and racist and classist subconsciousness of the liberal society shaped through the media and access to it?

Any suggestions?

I'm sure you won't have any because it is just the nature of the capitalist and bourgeois media flow. And that is what must be hacked and changed to make it visible and questionable. Only once something can be seen will we realise what has been invisible before. That's why we need to hack into media and change its message flow and the stereotypes it communicates.

But that should by no means be the ultimate goal.

What is lacking is a concise theory of what bourgeois society is like and what should be attacked by us. As long as you simply play around with the media - even as a media pirate or hacker - you are still part of the system. You have to change the political economics of a society. Otherwise, we will just be going round in the same old circles as the history of guerrilla communication clearly shows. Looking back at the guerrilla communication movement, it becomes clear that these strategies were an early form of viral marketing for the rebels themselves. A great part of the movement has made it to the top of our society and its institutions - like the former German minister of foreign

affairs, Joschka Fischer, once a notorious player in the huge Sponti-movement in Frankfurt before turning into a complete butthead.

So in the end, it is all about success. Success is what you want, isn't it? If so, do me a favor and erase all the information I just gave you. Maybe not sharing the information would be the utmost guerrilla communication act.

Johannes Grenzfurthner is an artist, writer, director, and DIY researcher. He founded monochrom (an internationally acting art-tech-theory group) in 1993. He is head of Arse Elektronika (sex and tech) festival in San Francisco and co-hosts Roboexotica (Festival for Cocktail-Robotics). He holds a professorship for art theory and art practice at the University of Applied Sciences, Graz, Austria. Recurring topics in his work are: contemporary art, activism, performance, humour, philosophy, sex, communism, postmodernism, media theory, cultural studies, popular culture studies, science fiction, and the debate about copyright. http://www.monochrom.at/english/

Granny Loves Linux!

by Metaranha

Those who are educated in a higher level of computer use (i.e. readers of *2600*) are already aware of the majesty and power of Linux. Slowly, the rest of the world is coming to understand those factors as well, but the question of which demographic to target with Linux and its variants is a little bit hard to hit. This article will not try to make any wild suggestions on who to give Linux to, but will instead offer interesting insight into two people who have chosen to live with Linux and are doing very well in their life after Windows.

About 6 months ago, I installed Ubuntu Linux on my mother-in-law's computer. My wife's parents are in their mid 50s and take a hard line against using computers at home, partly because they have to interact with them so frequently at their workplaces, and partly because working with computers is far from their forte. Finally, they were forced to give in to the demands of the modern world and asked me to set up my wife's old computer for them. The old Dell GX 260 was in dire need of a new operating system and, having no extra Windows disks around (coincidence?), I suggested that they give Linux a try.

I sat down with the wife's parents, gave them a very quick "how to," and away they went. It didn't take long at all for both of them to pick up the computer and do what they needed to do. Their computer is still working as good as it was the day I installed Linux, and they have had very minimal problems with using it.

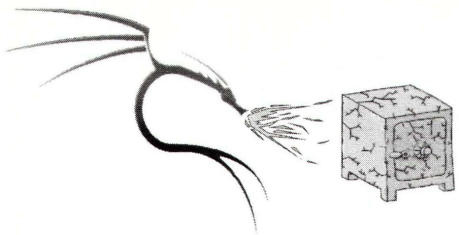
Recently, my boss asked me to take a look at his mother-in-law's computer. We will call her Mrs. N. I was only told that the computer was slow. Being that we've got a recession on, I acquiesced for the extra hours and left home bound for an elderly stranger's house. Mrs. N is in her mid 70's, and has an HP computer that was made within the last year. He instructed me to take company copies of Microsoft Office XP and Windows XP Professional.

I took my Hardy Heron live cd, arrived at her house in the afternoon, and asked her what types of problems she was having. My question was answered with the appearance of the Windows Vista loading screen. She told me that she didn't use the computer for anything besides Internet access, pictures and writing documents from time-to-time.

There was no reason why the hardware shouldn't work right, so I threw in the live cd and asked Mrs. N to take a seat and see what she thought. "It works a lot like Windows..." I said, and followed up with "...but it doesn't work anything like Windows."

I gave Mrs. N the same quick Ubuntu tour that I gave my previous "apprentices" and she took to it fast, but I didn't know if I had sold it well enough yet. I told her, "Look at it this way, you're going to be learning something new anyway. It will either be Windows Vista, or Ubuntu Linux. With Linux, you won't have to worry about viruses or spyware, and all of the programs you may need to use in the future are free, along with the operating system." "Free you say?" she asked.

One week later, Mrs. N's love for Linux is still rolling strong. The point here is to not underestimate the power of the casual user and elderly demographics. So the next time you visit grandma, take a copy of Ubuntu, or Suse, and have her give it a try. It's not going to be hard to convince her to use it full time, and you'll save your dear old granny the headache of using and maintaining Windows when all she wants to do is see pictures of her family and talk to you.



CRACKING WPA - PSK

...with Aircrack-ng & backtrack 3

by Mister Cool

WPA/WPA2 is a leading method of securing one's wireless network. It is well documented that WEP is, by design, vulnerable to various types of attacks. I would like to share with you today a method of cracking a WPA-PSK password on a wireless network.

The main tools utilized are Back Track 3 (aka BT3, a live Linux security distribution *freely* available at `http://www.remote-exploit.org/backtrack_download.html`), and the Aircrack-ng suite (a set of tools for auditing wireless networks, included in the live CD pre-installed).

First, a little background on WPA-PSK. Many home and small office users today utilize the WPA (WiFi Protected Access) - PSK (Pre-Shared Key), aka "Personal," option to secure their wireless networks. The Pre-Shared Key is a password or passphrase created by the administrator of the network, generally ranging from 8-63 ASCII characters (although it can be 64 hexadecimal digits). This plain text password (also called the Master Key, or key) is mixed or "salted" with the wireless network name (aka the SSID "Service Set Identifier"), to create a 256 bit value called a "hash." This hash value, commonly referred to as a PMK (Pairwise Master Key), is shared between an Access Point and a client, and will essentially be used to allow for the encryption of all network traffic.

In simple terms, WPA is basically a security protocol and the PSK is a password/key.

(For more on how hash functions and keys work, see `http://www.xs4all.nl/~rjoris/wpapsk.html`, `http://tldp.org/HOWTO/8021X-HOWTO/intro.html`, and `http://sid.rstack.org/pres/0810_BACon_WPA2_en.pdf`)

Most wireless networks use what's called an Open System Authentication to connect to an AP (Access Point). The steps are:

1. The computer asks the AP for authentication
2. The AP responds: OK, you're authenticated
3. The computer asks the AP for association
4. The AP responds: OK, you are now connected

What's known as a "four-way handshake" occurs during this connection process when utilizing WPA, and is what enables us to perform a WPA crack. The more specific term for what happens during the handshake is called EAPOL (Extensible Authentication Protocol) authentication and, if WPA is in use, you will be denied at step 2 without the password. (Please go to `http://www.wi-fiplanet.com/tutorials/article.php/3667586` for details on different types of wireless protection, and for an exacting explanation of what occurs during the four-way handshake process.)

The method of cracking a WPA password is slightly different than that of cracking WEP (Wired Equivalent Privacy). All wireless networks transmit data packets through the air. For a WEP crack, we would need to capture a large number of these packets (usually at least 40k-85K) which contain the IVs (Initialization Vectors) necessary to break the WEP password. Unlike WEP, in WPA the *only* thing that will enable us to even start the attack at all is what's called the "four-way handshake" between the client and the AP. Collecting more packets after we capture this "handshake" *will not* increase the chances of successfully recovering a WPA password.

The main method of attack with this type of wireless encryption is ultimately a standard dictionary attack. The WPA password can *only* be found if there is an *exact* match in the dictionary (aka wordlist) you are using. There are many wordlists and dictionary files available out there, I utilized a wordlist I found within Back Track 3 for this tutorial. (Visit `http://packetstorm security.org/Crackers/wordlists/` for a robust selection of freely downloadable wordlists.)

A WPA key is only as strong as the user who sets out to make it. And therein lies the weakness in WPA: The human element. If the password is a common word in the dictionary, it is very possible to recover. If a password is aardvark, it will probably be found when we implement a dictionary attack. If the password is aardvark1, the same dictionary attack will most likely fail as the "1" is not likely to be found in most wordlists.

The single most important thing to remember when attempting a dictionary attack is this: The attack will *only* be as good as the wordlist/dictionary file you use. If the password is not in the wordlist, you will *not* crack the password.

A WPA-PSK key is a required minimum of 8 characters long and, though we could attempt a brute force attack, it could take *hundreds* of

years to crack, even at that length, depending on factors such as the power of the computer, upper and lower case letters, numbers, and special characters. For a sample brute force time calculator visit http://lastbit.com/pswcalc.asp.

The main difference between WPA and WPA2 is that WPA uses the older TKIP (Temporal Key Integrity Protocol) encryption type scheme, while WPA2 utilizes the newer AES (Advanced Encryption Standard) encryption scheme which employs CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). (For details on CCMP, visit http://www.pcmag.com/encyclopedia_term/0,2542,t=AES-CCMP&i=37582,00.asp# and http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci1319465,00.html)

WPA and WPA2 personal are essentially the same for our purposes, as the method to recover these passwords is identical. (See http://www.networkworld.com/columnists/2006/091106-wireless-security.html?page=1 and http://www.openxtra.co.uk/articles/wpa-vs-80211i.php for a more detailed explanation of WPA vs. WPA2)

Now, Let's try our hand at cracking a WPA-PSK encrypted Wireless Network with this simple exercise. In this particular example I used:

1. A Toshiba Satellite L35-S2151 Laptop as the attacking PC (any computer with a supported wireless card should work)
2. An Atheros pre-installed wireless card (model AR5005G , many other cards are supported, see http://www.aircrack-ng.org/doku.php?id=compatibility_drivers)
3. The Back Track 3 Live CD
4. A target AP transmitting through a Linksys WCG200 Cable Gateway
5. Dell Inspiron 1000 as the client associated to the AP (aka the "client')

Our goals:

1. Set the wireless card in Monitor Mode with airmon-ng
2. Sniff for networks with airodump-ng
3. Find a client associated with the target AP, and start a capture file with airodump-ng
4. Deauthenticate the client from the AP using aireplay-ng and, upon client reconnection, capture the WPA handshake
5. Use the capture file containing the handshake in aircrack-ng to find the key

Now to the Good Stuff:

Start your computer with the Back Track 3 Live CD, and open a command shell (lower left tool bar, second icon in).

1) Set your card in Monitor Mode. This is necessary to allow your PC to listen to every wireless packet. This monitor mode also allows you to optionally inject packets into a network. Injection is useful to create network traffic if the network is not particularly busy. Injection is not absolutely needed to capture the handshake, but I have found it helps in finding associated clients. First, to stop the wireless card at the command prompt type:

```
airmon-ng stop ath0
```

Where ath0 is our interface (Atheros wireless card). Next, to start the wireless card in monitor mode type:

```
airmon-ng start wifi0 6
```

We must use "wifi0" instead of "ath0" as we are using the madwifi-ng drivers which are specific to the Atheros cards. The "6" at the end is the channel the card will operate on. We generally want to match this to the channel of our target AP. The output should indicate the interface ath0 is now in monitor mode. f

2) Now, to see what networks are out there, type:

```
airodump-ng ath0
```

This will show all the networks in range. The output will look something like:

```
CH  3 ][ Elapsed: 52 s ]
➥ [ 2009-01-18 21:28
 BSSID                PWR
➥ Beacons    #Data, #/s  CH
➥ MB  ENC  CIPHER AUTH ESSID
 00:18:F9:1A:13:30   35
➥ 244        4    0   6  54
➥ WPA  TKIP   PSK  linksys
 00:1D:7E:2C:E7:BF
➥ 23       109        3    0   11
➥ 54  WPA2 CCMP   PSK  2600
 00:1F:90:E3:19:26    7
➥ 18         1    0   1  54.
➥ WEP  WEP          NETGEAR
 BSSID               STATION
➥ PWR   Rate  Lost  Packets  Probes
 00:18:F9:1A:13:30
➥ 00:12:50:47:1A:DA   32
➥ 54-54      0        15
```

Where, notably: BSSID (Basic Service Set Identifier) = AP MAC address; Station = client MAC address; CH = channel of AP (note the CH in the upper left will be hopping, this is showing the channels that are being scanned for networks); MB = Network Speed (54 is wireless G); ENC = the encryption type, usually: OPN (open), WEP, WPA ,WPA2; CIPHER = the cipher used (WEP,TKIP,CCMP), usually TKIP with WPA and CCMP with WPA2; AUTH = authentication used (we're looking for PSK); ESSID (Extended Service Set Identifier) = Network Name (sometimes referred to simply as an SSID). As you can see, there were 3 wireless networks found. We are in luck as we have an associated client on the "linksys" network to target for our attack.

Optional: If you wish to do an injection test open a new shell and type:

```
aireplay-ng -9 ath0
```

I often use this as it sometimes causes associated clients not showing in our output to show up. If successful, you will get as part of the output message: `Injection is working!`

3) Next, we want to focus on our target AP. In this case, the "linksys" network. Open a new shell and type:

```
airodump-ng -c 6 -w capturefile
➥ --bssid 00:18:F9:1A:13:30 ath0
```

Where -c = channel of the AP; -w = the capture file (any name will do, in this case "capturefile"); --bssid = target AP MAC Address; and of course ath0 = our interface. The output will look almost the same as our original output above, but with just the one AP showing. The captured information will be saved to our capture file, located within the "Home" icon on the desktop.

4) Now, we need to capture the handshake. We will attempt to deauthenticate the client from the AP and, when it reconnects, we will capture the handshake! Open a new shell and type:

```
aireplay-ng -0 5 -a 00:18:F9:1A:13:30
-c 00:12:50:47:1A:DA ath0
```

Where -0 = the deauthentication attack; 5 = the number of tries for the deauthentication attack (I have found good success with 5, but this can be any number. However, too high a number may cause the client to fail to reconnect!); -a = AP MAC address (bssid); -c = client (Destination) MAC address; and ath0 our interface. Be patient, sometimes the output will indicate that the interface (ath0) is on a different channel than the AP. If this is the case, keep trying the command. You will eventually get the interface and AP on the same channel. Further, once the command runs, it does not always immediately capture the handshake. You may have to enter the command more than once. A successful capture of the handshake will show in this case as: `[WPA handshake: 00:18:F9:1A:13:30]` in the upper right corner next to the date and time of our original output screen.

5) Now for the crack! Open a new shell and type:

```
aircrack-ng capturefile-01.cap -w
➥/pentest/wireless/aircrack-ng/
➥test/password.lst
```

Where capturefile-01.cap = the capture file; -w = tells the program to run a wordlist; and /pentest/wireless/aircrack-ng/test/password.lst = the location of a wordlist that is included in the aircrack-ng suite for testing. This dictionary file is not very big, but suitable for our testing purpose. If the key is found the output will read similar to:

```
KEY FOUND! [ password ]
```

In this case the WPA-PSK password was "password" and we cracked it! (For more detailed information on the entire aircrack-ng suite visit `http://www.aircrack-ng.org`)

Sometimes the dictionary files themselves are huge, and the cracking process can take hours, even days! But the computations can be sped up by pre-computing the original hash value (the PMK we discussed earlier). This is easily accomplished by using either coWPAtty (included on the BT3 CD, see `http://wireless➥defence.org/Contents/coWPAttyMain➥.htm` for more details), or using a "special" form of Rainbow Table.

A Rainbow Table is a lookup table (similar to a multiplication table) that can be used to recover the plain-text password from a password "hash." These tables employ a time-memory trade off, in that the potential hashes are all pre-computed, so that they do not have to be calculated during a dictionary attack. This pre-computation drastically decreases the amount of computing power and time needed to find the correct key. The only caveat is that the time must be spent to do the initial pre-computation. Simply put in reference to these tables, it's much easier to do the calculations for the hash values once and store them for later use, than it is to calculate them every time they are needed. (See `http://www.freerain➥bowtables.com/faq/` for more details on how these tables work.)

Note that a traditional Rainbow Table will not work to crack a WPA password, as the original hash value is salted with the SSID. A set of hashes can *only* be pre-computed for one specific SSID at a time with any given dictionary file.

If the network name (SSID) was "linksys," and the dictionary file was "wordlist.txt," the pre-computed hashes would *only* work utilizing another SSID of "linksys." If the SSID was "2600," then the same pre-computed hashes will not work.

This is why the Church of WiFi has pre-computed hashes in what they call a "special" Rainbow Table (actually a PMK lookup table) against a 172,000 word dictionary for 1,000 common SSID's. While these files are rather large ranging from 7GB-33GB, they can dramatically decrease the time needed to find the correct password. (See `http://www.renderlab.net/projects/➥WPA-tables/` for more information on these tables.)

In conclusion, this is just a simple penetration test of WPA-PSK encryption. While not impenetrable, it can be near impossible to break if the password is random enough. The main lesson to be learned is that if you use this type of encryption, you should make your password something not found in a dictionary and somewhat random, and your network will remain relatively secure. For now. There are several random password generators out there, try one of these out for maximum security (`https://➥www.grc.com/passwords.htm` or `http:➥//www.kurtm.net/wpa-pskgen/`). And if you use "password" as your key, then you might as well not secure your network at all!

Australia

Sydney - Robots and Dinosaurs
662 Princes Highway, Kogarah
http://robotsanddinosaurs.org/

China

Shanghai - 88 Spaces
1118 Changshou Road, Suite 9G
http://www.88spaces.com/

India

Bangalore - Protospace Bangalore
Number 6 MR Garden
2nd cross KEB Layout
http://protost.ation.in/

Indonesia

Yogyakarta - The House of Natural Fiber
Perum Soragan Permai Number 6
http://www.natural-fiber.com/

Japan

Tokyo - 4nchor5 la6
Hirose House 202, Shibuya 4-3-5, Shibuya-ku
http://456.im/
Tokyo - Tokyo Hacker Space
Meguro Dai Ichi Coop 118 1-14-15, Aobadai Meguro-ku
http://www.tokyohackerspace.com/

Malaysia

Johor Bahru - Hackerspace Johor Bahru
Jalan Damai, Taman Sri Setia
http://groups.google.com/group/hackerspace-johor-bahru

New Zealand

Christchurch - Christchurch Creative Space
Canterbury Innovation Incubator
200 Armagh Street
http://chchspace.nztech.org/
Palmerston North - ProjectSpace
60 Princess Street
http://www.projectspace.co.nz/
Wellington - MakerSpace
41 Dixon Street
http://makerspace.org.nz/

Peru

Lima - Yachachiq Labs
Calle Los Duraznos, Lote 4, Mz P, Urb Ceres II, Ate
http://scitechbizdev.blogspot.com/

HACKER SPACES OF THE REST OF THE WORLD

Vowels & Consonants

Building the Community

Dear *2600:*

My name is Tuyishime Aimable. I live in Rwanda. I joined the *2600* community a few months ago. I like what you are doing. The problem is that I can't attend any meeting or any other event because I live very far from you. So I would like to ask you if you could help me to grow in that community otherwise or help me promote the 2600 in my country.

Aimable

Contrary to popular belief, you don't have to live in the Western world or even have access to high tech in order to be part of the hacker community or to spread the enthusiasm of the hacker culture. If we look back at the really early days in our own country, hackers did just fine playing with rotary dial phones and glorified electric typewriters. While technology is often at the heart of it all, it's actually not just about the technology in the end. It's about the thought process. If you learn to think like a hacker, where you are and what you have access to will become secondary. By questioning everything - human or machine - and by constantly experimenting and sharing your findings, you'll be able to apply this hacker mindset to almost any situation and, in so doing, find other like-minded individuals. This is another reassuring fact. There are always other people, no matter where you are, who will share your curiosity and passion. It's just a question of reaching them. So our advice is to use this distance as an opportunity to start something fresh and to be a real pioneer in your country. Just because you're far away from us doesn't mean that you can't start running your own meetings or events. Of course, every country is different with regards to rules, what is tolerated, and how individual thinkers are dealt with. So make sure you're familiar with what you're up against and what you're willing to fight for. As hackers are almost always heavily involved in freedom of speech issues, the reaction against them can sometimes be a bit heavy handed. This is true of any authority figure. So be aware of this, keep reading a lot, and always maintain a level of curiosity. You will find the hacker community all around you.

Dear *2600:*

Hiya I'm 15 and love technology and love to talk about it. My question is am I able to attend the meeting in Dublin and what do I bring if I am allowed? Can you tell me a little about what we do at the meetings and what I need? What do I need to bring (laptop, money, etc.)? Thanks.

warlock

There are absolutely no requirements of this sort to attend one of our meetings. They're open to all ages and there's no admission fee of any type. We welcome people of all levels of expertise, including those who believe they know absolutely nothing. (In fact, we greatly prefer them to those people who believe they know everything.) All we ask is that you come with an open mind, help those who ask questions, avoid developing cliques, and be ready to explain what we're all about to those who might not get it right away, including any security guards who may work in the space you're meeting in. Some meetings have presentations but most are simply gatherings where people talk to a variety of individuals who show up. There will always be those who imagine the meetings exist for the purpose of obtaining illegal information or devices and you may even encounter attendees who believe this and who try to subvert the image of hackers into the mass media definition. This is why it's so important to understand what the meetings are really about and to invite people from all circles to join in and make them even better. We hope you find them interesting; the Dublin crowd is a good one.

Dear *2600:*

How can I find a hacker group or convention in South Florida?

Joel

We're not aware of any hacker conferences taking place in that part of the country and none of the four 2600 meetings in Florida are in the southern part of the state. We certainly hope something gets started as a result of your inquiry.

Dear *2600:*

I am working on starting a *2600* meeting in my local area (Silicon Valley). However, there are two fantastic meetings already in San Jose and San Francisco, about a 60 minute drive from where I plan on setting up the meeting (Moun-

tain View or Palo Alto). I'm ready to publicize it, but I was considering setting it up for the third Friday instead of the first of each month.

The reasoning behind this is because there are two great meetings already. I don't want to cut into them and make people choose, while at the same time give those who wouldn't want to drive into the cities (and deal with parking) or deal with the train schedules (which end before most meetings end). Furthermore, Palo Alto and Mountain View are the homes of many startups as well as Google, and I feel that such a meeting in one of these nearby locations would do quite well to bring people together.

If I do this, would that alternative Friday be acceptable in your opinion?

Lowery

Having secondary meetings in other places is a great idea. We understand that once a month often isn't enough but it's also good to get to other places and, in addition, offer people who can't get to a meeting in a major city an opportunity to meet other hackers. It just gets really complicated if we have to keep track of all of these meetings, so we try to keep it simple by only listing the "first Friday of the month" ones. Having meetings on the same day of the month makes it easy to keep track of and there's never a question of which day is 2600 Meeting Day. Obviously, there will always be people who can't make it to the meeting on a particular day but the first Friday rule has been in effect for over 20 years and it's reached the stage where it's factored into people's schedules before they accept a job offer or complete their class schedule. (At least for a few people it's gotten to that point.)

Dear *2600:*

I just got the guidelines auto-reply. I don't know why I didn't see that sooner (hint: I'm a dolt). That lays out some excellent points, and might put an end to my plans (which isn't necessarily a bad thing).

Lowery

Our auto-reply also explains the rationale behind having the meetings on the first Friday of each month. However, your idea is still a good one and there are already numerous meetings that have "unofficial" get-togethers in either the same or a different location. What we suggest is that you spread the word at the official meetings and see if you can get some enthusiasm for the alternative ones. Anything that helps to build the community is a good thing.

Dear *2600:*

First off, I wanted to congratulate you for making such a great publication available to the public for over 26 years.

I live in Bakersfield, California and the closest *2600* meeting is over 100 miles away in Los Angeles, so I'm considering organizing meetings here in Bakersfield if there's enough interest locally. Anyone interested should contact me through the form on the website: bakersfield2600.webs.com.

Jason

For those interested in setting up more meetings and reaching out to the 2600 readership in this manner, might we suggest a free Marketplace ad? You would need to be a subscriber or at least know someone who's a subscriber who could submit the ad. We imagine there are lots of potential areas for meetings but it's always a challenge to reach out to people when you have yet to meet them.

Dear *2600:*

I recently moved to Amsterdam and was astonished that there is currently no *2600* meeting here. How would I go about starting a meeting here? (I'm not sure there would be any interest.)

I've been attending *2600* meetings in Ottawa and Toronto for quite a few years now. I no longer hack hardware/code (software engineer now) but enjoy attending mainly because the people are so interesting at these meeting.

peter

It's hard to imagine why there would be no interest, particularly in a city as individualistic and creative as Amsterdam. Having the magazine available usually helps and it's possible that might be a challenge if no local bookstores are willing to carry it. Oftentimes though, the only reason a meeting isn't taking place in a major city is simply because nobody has yet taken the time to put one together.

Dear *2600:*

I am wondering if the staff of *2600* would be interested in having a website designed and implemented using a content management system such as Joomla. I would be willing to do all the work for free. My only motivation for doing this is to make the website more reliable, accessible, and easy to use for both the admins and the users. Any thought on this would be appreciated.

Thanks and keep up the great work!

Zach

Designing and implementing a site is a single step in a long process as there are countless things that can and will go wrong down the road. We're not at all discounting your generous offer but it's important to realize that such things are more complicated than appear at first glance. We actually have a number of people working to overhaul our site and we're confident we'll get there one day. Until then, if there are features that aren't working properly or things our site should be doing that it isn't, we would like to focus our attention on that in the more immediate future.

Dear *2600:*

Sir, I am a student and currently pursuing my B. Tech. degree. I am from India. I am sorry because I am going to ask you the same question which I think you hear a lot from the basic user: that is, how I can be a hacker. I know the differ-

ence between a hacker and a cracker. I surf a lot on the net to find the beginning but failed to find a real one. Sir, please tell me from where to start and which courses I should take. In short, how I can be a hacker. I know that I can't be hacker just in a night. It takes a lot of time and determination but sir, I don't know from where to start.

Please give attention to my request. I will be very thankful to you.

Prateek

We get so many requests like this and it's important to make it clear that hacking isn't something that is taught like a class. It's a state of mind and you get there by experimenting and asking a whole lot of questions. You obviously need to have an interest in the stuff you're asking questions about. You need to not be afraid to step out of the rigid confines of rules and see what happens under different conditions. Don't buy into the hype of hacker versus cracker and the silly colored hat designations. Being a hacker means to be someone with a strong desire to learn and to innovate. What you do with that knowledge and ability later on is a totally different story.

Ideas on Spreading Knowledge

Dear *2600*:

I'd like to suggest a topic for an article. The topic would be a guide to the North American phone system for newbies, and would start by describing the dial plan.

For example, like most other people, I thought the "one" you dialed before a long distance number was the "long distance access code." According to the O'Reilly book *Asterisk: The Future of Telephony,* this is mistaken. The "one" is actually the "country code" where the "country" in question is the NANP (North American Numbering Plan), which includes the U.S., Canada, and some Caribbean countries. They are distinguished by the familiar three-digit area codes (called NPAs). Within the NANP system, dialing 011 indicates an international number. This is how you dial countries outside the NANP.

That's really all I know. Someone with more knowledge, pick it up and run from there. It would be a boon to everyone who isn't already a phone phreak.

Travis H.

The phone network is what inspired a great many hackers to start exploring in the first place. It's filled with all sorts of fascinating details and trivia, and most of what you explain above is accurate. However, you're not dialing a country code every time you precede a domestic number with a "one." That's just the (somewhat outdated) method of indicating that you're dialing outside your area code or making a long distance call. We've had articles on this subject in the past but are certainly open to printing new ones with updates and additional information.

Dear *2600*:

I'd like to write about creating web2.0collage.com (namely how the browser history sniffing worked, how the scaling worked when it got on Slashdot, and a bit about the potential privacy concerns). Would something about this be of interest to you?

Holden

Most certainly. The concept of a page that shows a collage of websites a user has visited by digging through their browser's history is fascinating, creative, and frightening. Those can be considered our three essential ingredients.

New Information

Dear *2600*:

I wanted to add to the advice you wrote in response to dawn's letter in 26:2 about how to try and get out of her cell phone contract. You suggested that she could downgrade her plan, but I wanted to let your readers know just how far you can downgrade. My sister recently wanted to switch carriers but had eight or so months left on her contract, so she called her carrier to find out what they could do for her. The CSR she spoke with informed her that, rather than pay the early termination fee, she could downgrade her plan to an obscenely low-priced (and massively neutered) $10 a month plan instead for the remainder of the contract period. She would just have to be willing to give up her current number and get a new one with her new carrier if she still wanted to switch, since the current number would still be "active." She was able to effectively pay only $80 for the remainder of her contract period rather than the $150 it was going to cost her to cancel early, and she's been happy with her new hardware and service on her new carrier ever since. With luck, this information can help anyone who finds themselves looking at the green grass on the other side of the fence, whatever field they may be in.

dmchale

Dear *2600*:

Since *2600* seems to be a sociopolitical magazine, not just a technical one, I wanted to send you and your readers this information.

The documentary *The Obama Deception*, directed by Alex Jones, theorizes that Obama won because he was seen as most acceptable to the public and the people who apparently always run the government. It's available on YouTube.

The documentary *ZERO: An Investigation Into 9/11* directed by Franco Fracassi and Francesco Trento has some interesting claims about what happened on September 11, 2001. It's available on Google Video.

If you are interested in these types of things, try browsing *The Reality Zone* (http://realityzone.com).

This letter sounds like a shameless plug, but even I think some of the ideas in the documenta-

ries and the site sound too surreal. I still have to check the claims.

Happy watching (and reading).

katkat

Conspiracy theories are always interesting and fun to watch, as long as you question them as much as whatever it is they're questioning. After all, most conspiracy theories are part of the conspiracy themselves. (We're waiting for the documentary on that.)

Dear *2600*:

Vinicius K-Max is a well known Brazilian "computer enthusiast." (Is he a "hacker" or "digital prankster" - who knows?) Some time ago, he was in the news because he kidnapped some Orkut communities with an exploit. He hit the news again in the first Campus Party last year by redirecting the traffic of a LAN to his laptop. When people tried to access sites such as Google, Blogger, Flickr, Orkut, and others, he presented a fake page saying the organization considered the requested page to be an inappropriate website. That led to lots of discussions about security, the organization, and whatnot.

Now K-Max is in the news again, but in some serious trouble. He found a way to access private data from customers of the Telefonica phone company trough the Internet. He contacted the company about it, and also put up a website for anyone to verify this security flaw.

Now the company is accusing him of data theft. The police already have gone to his house, armed with guns, and taken some of his equipment. He will be indicted for "distribution of secrets," which means one to four years of arrest. K-Max says he only wanted to expose a security flaw in the Telefonica system. Apparently, they also want to indict him for his previous acts, too.

The country is right now in the midst of a controversy because of a proposed law to typify digital crimes, and other ideas regarding the Internet. And Telefonica is also not very popular because of some faults on their Internet service.

I doubt it anyone is pressing charges on the company.

It will be interesting to see what happens.

++divide_by_zero

It most definitely will be and we'll be keeping an eye on this. It just goes to show that there are interesting hacker cases going on all over the world and we would do well to pay attention to them at least as much as we focus on what's happening close to home. Thanks for letting us know about this.

All Sorts of Questions

Dear *2600*:

I was not really sure which email address to send this to but I wanted to get some information on submitting photos to the magazine.

I work for the Evil Empire (AT&T) and have access to pretty much all the systems, plant, MDF, switches, DSLAMs, etc. I get to see this stuff every day. I might just be a phreak but I believe some other people would like to see everything from the ancient equipment to the latest and greatest.

I would be more then happy to write up a small article on the piece of equipment that is in the photo as well. Thanks for your time and consideration and, as always, I will do it for just the gratification of helping others.

Brad

We look forward to receiving your submissions. This is a great example of how people within certain organizations - who have access to things we can only dream about - can make our world so much more interesting simply by sharing information. Thanks for helping to preserve the hacker spirit.

Dear *2600*:

First off: goodness! Did you really send that fellow every copy of *2600*? That would rock!

I am 14 years old and a budding hacker/phreak. But, really, none of this "teach me to hack" crap. No! I have decided to develop myself through reading and exploring with specific questions and answers.

I always download your radio show and have purchased a copy of your anthology. Good stuff!

Second (or third) off: Thanks. I really appreciate everything you folks there at *2600* do for me and everyone else. I have found the hacker community welcoming and informative. Thanks.

Random ballyhoo: how many people make up the staff there? Just curious.

Wow, that letter I just wrote *did* feel somewhat like conquering a mountain! Or taking down "the man!" Hooray!

Leone263

It sounds like you're on the right path. Thanks for writing. In answer to your query, it depends on what the definition of "staff" is. We have a handful of people who devote their entire lives to our organization (not counting all of the lunatics who do this without our knowledge), and then there are people who contribute what they can, whether it be through writing, taking pictures, lending expertise on a variety of technical and non-technical fronts, etc. The latter would be a frighteningly large number if we ever tried to calculate it. We suspect the authorities already have, which is why they live in constant fear over what we might do next.

Dear *2600*:

I want to place an order on your store and I would like to know if you ship to Australia. My method of payment will be credit card. So please let me know if you can assist me with the order. And please do not forget to include your web page in your replying back to my mail.

I will await your prompt response as soon as you receive this mail. I will be very glad if you treat this email with good concern.

Frank Moore

This one almost got us but it actually is part of a scam. The "good concern" is what seemed a little fishy so we checked online and, sure enough, there are thousands of almost identically worded letters floating around on the net. What's the scam? Well, first of all, printing our reply in a magazine pretty much defuses the whole thing right away. However, were we to respond to this person via return email, we would undoubtedly get a followup asking for a list of products we sell. (That in itself is a bit strange since someone should already know this if they're interested in ordering something from us.) They would then send an email ordering a large number of items, and somehow the only way to make the order go through would be to involve bank transfers to third parties once their payment to us had been received. We would be enticed by having the amount they pay to us be substantially more than what we needed to transfer to the third party, most likely an additional amount for our "trouble." Needless to say, their payment to us would turn out to be fraudulent and any money we sent out would be lost along with anything we sent them in the mail.

It's hard to imagine people falling for such schemes but it happens all the time and the fact that even for a moment we thought this was a real letter indicates that these con jobs can, in theory, still work.

Incidentally, yes, we do ship to Australia.

Dear *2600*:

First of all, I recently subscribed to *2600* and I love it.

I was thinking of starting my own small quarterly magazine and was wondering if you had any advice. Thanks!

Michael

We assume you're talking about starting an actual printed magazine as opposed to something online. Going print is a lot harder and has many challenges but we find the printed word is more enduring, if only because it requires a certain commitment that oftentimes doesn't exist in the glut of electronic prose. Naturally, there are exceptions on both ends of the spectrum but print is in our blood so we're naturally going to feel its magic.

The best advice we can offer you is to let your zine grow into a rhythm. Most new zines either overdo it and get burned out (or lose a ton of money) or don't put in enough effort and wind up never really going anywhere. You need to gauge your readership and figure out where your content is coming from and how much of it you can manage for each issue. These things take time and you will almost certainly not get it right from the start. The important thing is to realize that you will be putting effort, money, and material into this project and you may never wind up in the black. If you can accept that and work it out so that in the worst case scenario you don't lose a fortune, then you have a much better chance of evolving into a regular publication that might, at the least, break even. But, no matter what, having that printed object in front of you is an achievement you will be proud of for many years to come. That's why it's always better to try and fail rather than avoid failing by not trying.

Dear *2600*:

PLEASE I NEED TO KNOW IF YOU HAVE TO CALL TO CUBA, GOOD RATE.

Nicolas

Why on earth do you think we're the people to ask about this? Go shop around, ask Google, visit a corner grocery that sells phone cards, participate in online forums where people actually discuss this stuff, or ask random people on the street. You also might want to find a way to unstick your caps lock key. Good luck.

Dear *2600*:

If I want to get more information on the phone systems nowadays, where can I get it? Or where should I start?

Apple Freak

A good place to start is by defining your terms. There is no one phone system obviously but there are so many different aspects to phone networks today that it's hard to sum it all up with one label. Voice over IP is one category that has almost infinite worlds of possibility. Or perhaps you're interested in private networks (PBXs), the more traditional long distance phone companies, how the switches themselves are wired together, or maybe just some history on how it all used to be. You can get a lot of info just by asking, whether that be in the letters section here, on some sort of online forum, or by meeting other like-minded people at conferences or 2600 meetings. Of course, exploring your local bookshop or library is another great way to learn. And don't forget the method so many of us used to figure it all out - hands-on access. Every phone everywhere is a portal.

Dear *2600*:

In the recently published *The Best of 2600* book, there is a mention of a 1991 video covering Dutch hackers accessing military computer systems in the United States. Is this video still available?

iphelix

That video hasn't been available for some time but you can expect it to rear its head as we digitize some of our older material.

Dear *2600*:

I just came back from Mauritius (very small island in the Indian ocean) and took pictures of two different payphones for you. They were taken with a 12MP SLR so they are five megabytes each. Should I email them together or separately, or should I upload them to a specific place? I don't want to blow up any mailboxes.

Also, when I send the pics, should I include a caption with each?

Scott Brown

Since one of your pictures is appearing in this issue, we trust you found the answer. For everyone else, don't worry about size (however, images that are too small won't print well), and please provide as much info as you can on the phone being submitted: where it was found, any interesting facts, etc. The email address is payphones@2600.com.

Dear *2600:*

FYI in case you've not gotten this yet. Do you have any idea who/what this is?

---------- Forwarded message ----------
Sent: Sun, 19 Jul 2009 11:06:51 -0400
Subject: OperationUtopia

Just got this e-mail & thought you might be interested. I ran a search for e-mail addresses associated with 2600 articles. Pass it on or check them out-you may not believe what they have going on.. ...Due to the threat of gov. controlled public manipulations through cyberwarfare & cyberattacks, an independent non-national group of hackers has sprung up. Whether things like the recent DoS attacks on the Pentagon, which media outlets claim came from North Korean sympathizers are real is a moot point. If there is no independent arbitration & things like this go unchecked networks will become locked down as a response to this cyberterrorism, no matter who the real terrorists are. As well, reactionary defenses from these types of threats to net neutrality & freedom on the net will be to late. A proactive approach must be taken. This group, who some have called the secret society, is gearing up to launch a global alternate reality game where everyone who comes into contact with them will be working on a project called Operation Utopia. From the outside oputopia looks like a game whose solution is figuring out what the secret society really is. In actuality it is distributive hacking, & if enough people play the game they will have a workforce unparalleled in recent history. I have heard they communicate via encryptions based on the non triuial zeros of the riemann hypothesis. Heavy stuff. Anyway get word to as many hackers as possible, if not to support the secret society, at least to investigate them & question their motives. For them to have remained anonymous for so long is remarkable from what I hear they have done & who is with them. operationutopia@hotmail.com is a contact point. Forward all this info to as many hackers as possible. If these guys are for real it will change everything.

----- End forwarded message -----

Sai

No, but you've thoroughly spooked us out. How ever did they find out our secret plans?

Dear *2600:*

Would you have any photographs or information on the payphones that would have been in use during 1970-1975 in Vietnam? I am researching props for a production of *Miss Saigon* and would love to be as historically accurate as possible.

Thank you for your time.

Steven

As that was a fairly chaotic period in the country's history, it might be difficult to find actual photos of payphones with much attention to detail. We can say almost certainly that any phones submitted to us in recent memory would be of a very different style than those in use back in the 1970s. However, our readers are a tremendous resource so if there is an answer to your question, we will hear it from them. We'll keep you in the loop.

Dear *2600:*

I have read on your site very nice things but I can you help me please with some hacking. Its about a betting site and they have in every betting house a TVs on them are going recorded dog bets 1-6 my question is can we hack them to see whats next bet on dogs there is a lot of money to win can you answer me please bye :)

Arnel

You want us to somehow help you hack dog betting? Other than fixing the races (let's hope you're talking about races), what precisely do you think we can do? We'd like to say this is the most unclear letter we've ever gotten but it wouldn't be true - not for this issue and not even for the day that this was received. We seem to have become the clearinghouse for the dazed and confused.

Dear *2600:*

I am a 53-year-old woman and only child. Both parents are deceased. I have no husband and no children. My father was career USAF and reached full colonel. I live in my parents' home, which I inherited. I am retired after 30 years of teaching. I own a Dell laptop running XP and an older desktop running Win 98SE. The desktop is run off-line and my laptop is used almost exclusively for email.

I've read your magazine off and on for years. That, and being an Air Force brat, prompts me to ask the following questions. First, based on what I read in *2600* every quarter, give me one good reason why I should use a wireless anything? Second, since it's a *fact* that extraterrestrials have visited Earth on countless occasions and that the United States is in possession of a vast amount of advanced extraterrestrial technology, why should I participate in the ongoing technological charade, or for that matter, every other charade that Americans suffer from our government? Thanks for publishing *2600*.

Julie

Let's tackle your first question first. Sometimes wireless things are more convenient. Phones, computers, radios all can be used with more

flexibility when there are no wires involved. But in the case of wireless devices that transmit, the health effects are still somewhat unknown, mostly because these devices haven't been around that long. There are also security concerns if proper precautions aren't taken with regard to protecting content. You can certainly survive just fine without using wireless technology if you so choose. Now to your second question. We have no comment at this time.

Dear *2600:*

I have an interesting issue regarding letter submissions. First, I would like to know if you actually accept letters. Of course you accept emails, but some people may be confused about this terminology. I also would like this clarified before I spend my valuable time writing something in a format your magazine may consider obsolete. I know you guys would gush over a real written letter, but it might not do me any good in getting it printed in the mag.

For me, a letter can be two things: something written out by hand or something that is typed up, printed out, then sent through the mail. My question is this: What if someone were to write you a letter by hand or type it up and send it through the mail and you wanted to print it in the magazine? Would someone at the office type the letter up on the computer? What if it was a lengthy letter? I think clarifying this would satisfy the dwindling number of us who still value this timeless form of communication.

Being creative by nature, I value tangible things much more than I value seeing information on a screen, just like when Emmanuel Goldstein states that the printed word is still the most valuable form of communication. Sure I hack, play video games, and text. But I also draw, write, and travel. In other words, I cater to the desire to see and touch real things.

I recently purchased a fully restored typewriter from the 1930s from an online store. To say that typing on it was a humbling experience would be a severe understatement. It gives me a feeling of nostalgia and excitement that I can only compare to receiving the latest issue of *2600* in the mailbox.

When was the last time any of us sent or received a real letter? It's been too long. Write a note to your buddies congratulating them on a good business meeting! Write your girlfriend and thank her for last weekend! Write to an incarcerated *2600* reader! Put down that Blackberry and pick up a pen!

For me, an old fashioned typewriter has just the right amount of technology. My typewriter never gets viruses, never has to be restarted, and never crashes. The operating system never needs to be upgraded and I don't need to worry about registering it with the company I bought it from. It has an infinite amount of storage space because I can always purchase a new box of paper. And when I walk away from typing, I don't have to worry about draining power and can pick up right where I left off. Find me a computer that still works after almost 80 years.

We can't be creative as hackers if we don't understand the technology that got us to where we are today. Don't get so engrossed in staring at screens that words on paper don't mean anything to you. Good luck to all in reconnecting with your creative side.

As a final note, this "letter" was really an email to *2600*. I'm not going to write or type a real letter until I know how *2600* will print it in the magazine.

Thanks again for a great magazine!

sc0ut

If the letter or article is interesting and informative, we will print it. We regularly transcribe typed and handwritten letters and articles (the only way people in prison can communicate) and in the past we've even transcribed articles that were spoken into our answering machine. We weren't particularly happy about it, but it needed to be done. The point is that if it's something our readers will appreciate, we'll do whatever it takes to include it.

Dear *2600:*

I was banned from this site just because the admin got the bribe from one member and when I questioned him why he banned good members without giving notice and keep the bastard just because they kissed his ass and bribe him with gift card money, he banned me without notice too and deleted my thread to erase the evidence.

Do you think that you can hack this site? Cause they're always proud that they're well protected and back up frequently.

Let's see who's better.

Son

Yes, this is exactly the kind of thing we want to get involved in. Thanks for thinking of us.

Dear *2600:*

Hello. My name is Ray. I am visiting Honduras, and for way too long. A year too long. Is there any way that I can enter the Honduran database to alter my date of entry and my port of entry? Thank you for any help that you can give me.

Ray

So you'd like for us to erase a year off of your stay in Honduras? There's bound to be a good story in here somewhere and we'd really like to hear it. We have a hunch it might be a little more complicated than simply changing dates in one country's database. We'd probably have to change a second country's database too. And mess with the memories of the people who were supposed to have seen you for the past year. It could get a little tricky. And, oh yes, expensive. But we've said too much.

Dear *2600*:

Why *2600* don't have meeting in Malaysia?

Fiez

Just a guess but probably because nobody in Malaysia set one up. You are nominated, assuming you're actually in that country and aren't simply asking from somewhere else for some reason.

Interesting Observations

Dear *2600*:

I read the letter from Vandy in 26:1. He continues at length about what we know and don't know, and finishes with, "Thanks to *2600* for doing what you do, and helping keep us out of the camps." In the back of the mag, in the Marketplace, you advertise events for ToorCamp and HAR2009. Oh, the irony!

eddiehaskell

Dear *2600*:

I've been wandering around the skyways today and discovered a Coca Cola machine. An "Intellivend 2000" to be precise. It has a column of nine buttons used for choosing which soda you wish to buy. Haven't gotten it to dispense the soda for free yet - I have to figure this out, though. If we label the column of nine buttons 0-1-2-3-4-5-6-7-8, you can press 0-3-1-2-0 to get into a menu. 0 becomes "back", 1 becomes "up", 2 becomes "down", and 3 becomes "select". Root menu, as shown on its little red LED display has "eror", "rbn", "ubr", and "sale". You can press up and down to select between these and press 3 or "select" once you have one that you want. Selecting "eror" gives you "sts" and selecting that gives you "da" one through twelve. Don't know what these are. Selecting "rbn" doesn't do anything. Selecting "ubr" displays "67015-6". Don't know what this is. Selecting "sale" gives you "0002-6655" and selecting that gives you a choice of viewing "sl" one through twelve. I guess these are sale counts but there are only nine sodas to choose from - 10, 11, and 12 were all "0001" on the machine that I was looking at. The rest were a bunch of different numbers. Unplugging the machine and replugging it back in didn't change anything in the menu. If anyone can do this too, write in. I looked around for the same model machine so I could try it on two vending machines, but I couldn't find any. Next time, I'm going to experiment with holding down buttons and unplugging/plugging it back it in.

sigflup

Finding a manual online for this particular model or simply trading information with other people who have access to this machine shouldn't be too hard. In fact, most interesting machines have documentation that would make really good articles if translated from manual-speak.

Dear *2600*:

I have been in the electronic security industry since the early 1990s, at first installing and later designing and selling CCTV, access control, intrusion, fire alarm systems, and integration packages. I think that your fine magazine should be mandatory reading for anyone who works in any security field. I've been a reader for so long that I forgot when I started.

All of our security systems have a computer/network component. It always amazes me that my industry "peers" seem to know so little about computer networks and less about network security. I always ask people in my business if they read or know what *2600* is, and the answer is almost always no. It is no wonder that IT managers cringe when they see us pulling into their parking lots!

I want to remark on an editor's response to a letter by Estragon in the 26:1 issue concerning CCTV systems in supermarkets. This same remark can be applied to many surveillance system installations.

Large CCTV installations in supermarkets are very common. Many "mega-stores" may have 64 or more cameras and four or more DVRs connected to RAID arrays to collect and archive video (to be stored for years in some cases). The reason is not to stop you from shoplifting a steak or some dairy products, although this deterrence is a side benefit. The main issue is the store protecting itself from fraudulent "slip and fall" personal injury lawsuits.

You have to sell a lot of lettuce to buy a $30,000 to $40,000 CCTV system, but if you prevent one fraudulent lawsuit, the system has paid for itself many times over. Supermarkets which operate on a notoriously low profit margin are able to win discounts on insurance for having these systems installed. Video images are sometimes stored for the length of time allowed to file a lawsuit against the store. This is years in many localities. Hence, the RAID array.

Reading a book by its cover can be misleading. In the example shown here, the motive is purely economic (could even be greed). Yes, storing images of shoppers (including me) grates on me, but in many cases, these stores need this protection to stay in business.

Just thought a view from a different angle might be enlightening.

The Security Department

We thank you for showing us a different perspective on this.

Dear *2600*:

It appears that some "hackers" play golf but may not in fact be technology enthusiasts!

I know the back cover photo is supposed to be something in real life, but I ran across this site, complete with its "Hacker History" and "Hacker Factor" (yes, of course (double pun!) the pun was intended), and couldn't

help but share the URL with the rest of you: http://www.austinhackers.com

However, if you are/were looking for the other kind of hacker, check out: http://wiki.austinhackers.org

Golden Helix

Scary, ain't it?

Dear *2600:*

My subscription lapsed and I went to my local Borders to pick up the newest issue. It took me about 15 minutes to find it. It was stuffed behind a stack of *Macworlds*. I took the few they had and put them in the wire cage on the front of the shelf.

Another thing, the old man at the counter couldn't ring it up. He tried about 20 times but it just didn't happen. He then just gave it to me free. I didn't want to complain (I mean, who doesn't like free stuff) but I thought it harmful to *2600*. I brought it up to the man and he said "Oh well." So I took it. Just letting you know.

UncleJesus

This kind of thing happens all the time and yet we still get charged by stores for "missing" issues as if it were somehow our fault. It's yet another example of how publishers are getting screwed by a monopolistic industry.

Dear *2600:*

I heard a news bulletin on BBC Radio 2 state that the British government's National Pandemic Flu Service website went down after receiving 2600 hits per second. This frequency rings a bell for me. Perhaps one of your readers knows where I might have heard of it before.

Mr. Fossey

Dear *2600:*

I owe you an apology. I've been a longtime reader, and though this is the first time I've actually submitted anything to you, I've composed numerous articles in my head. This, however, is not the reason for my apology. I have a very strong sense of both civil liberties and security, and have been flatly disgusted with the current security procedures used by U.S. airports. Being a frequent flyer, I always streamline my process to avoid hassle, although I definitely do penetration testing most every time I fly. There simply is no reasonable security system in place, but of course this we already knew. What we didn't know was that the carry-on I used for the first leg of my current flight had not been emptied since July 4th. Imagine my shock when, after arriving at my destination, I discovered an explosive, two electrical ignitors, and a flask (which could conceivably have contained anything) still in my bag. I even remember the security agent's smile to me as he saw me doing a professional check of my body for metal before going through the detector. Seriously, it was an incredibly irresponsible oversight on my part, and in hindsight I'm very grateful to be writing this from the return flight, rather than a cell. Obviously, I corrected the problem and expected a smooth process through screening, but this was not the case.

The incredibly slow and, as we know, useless scrutiny of every person's ID and boarding pass bottlenecked the lines, and, by the time I got my bag into the tub for screening, I was running late. My bag was deemed suspicious, taken out for inspection (twice, looking for nonexistent liquids), and run back through the machine twice as well. There were no liquids, no sharp objects, no electronics. Simply gross incompetence on the part of the security agents. My carry-on was now in several pieces, and here is where my apology comes in.

What had fallen out in front of the tub my bag was on? Rolling face up on the conveyor belt towards me, was my 26:2 issue of *2600*. You know, the one where cbsm2009 shows how simple it is to subvert airline security.... And I didn't get the picture in time.

I would say "keep up the great work," but honestly, after these many years of quality, if you feel like slacking off a bit, you deserve it.

Me

Sent from my iHack

Dear *2600:*

I am a new and avid reader, and might I say you are a breath of fresh air in the stagnating pool of puss that we call the mass media.

I just watched *Freedom Downtime* and I have been reading *The Best of 2600: A Hacker Odyssey*. I must say, I missed out on so much. Here I was back in high school from 1997 to 2001 just messing around with the computers, like running Windows in safe mode just to bypass the password login so I could try to get on the Internet and look up some SNES roms and Napster songs. I just wish I had found out about *2600* then. But here I go rambling on. I do wish I could of helped some way with Kevin back then.

You guys rock. Keep the First Amendment alive.

Levi del Valle

While you may have missed out on one bit of history through no fault of your own, remember that what you do now will form the next piece of the puzzle. There are constant changes going on in the world of technology and in how society handles it all. You can be a key part of that or an important element of something else altogether. There is magic in every generation as well as the ability for a single individual to effect significant change. The one factor that never seems to disappear is the constant reminder from those in charge that makes us feel as if we have no actual power. But nothing could be further from the truth.

Dear *2600:*

I recently traveled through the Denver airport. I wish I had taken a photo of a glass case with all of the items that are not permitted onto airplanes by passengers. They actually had a

small chainsaw in the glass case!

I was surprised at how easy it was to get my e-ticket from the kiosk. I did not have to show any ID or anything beyond entering a 13 digit number. Though lame, idiotic, or crazy, it seems fairly easy to impersonate a passenger if one has access to the 13 digit e-ticket number and a fake ID with the name that's printed on the boarding pass. And the boarding pass did not have an address on it, so when security checks the boarding pass and the ID, they will not have to compare addresses or faces, only the spelling of the names on the boarding pass and ID.

It would be pretty lame if someone attempted to impersonate a passenger for whatever crazed reasons, but I think it's just too easy and simple to print out a boarding pass by using a 13 digit number. Perhaps statistics on passenger impersonation incidents are not high enough to change anything, if those stats even exist.

JZ

If you have all of this information, know exactly where to go, and have even made up a fake ID in the victim's name, it seems you've already invested quite a bit of effort into getting someone else's ticket. We assume you also would somehow know that the person wasn't going to show up and cause a big scene which, unlike in the movies, would probably wind up with your little ruse being exposed. But let's say that you managed to pull it off. So what? Using an assumed name has nothing to do with security. At worst, all you would have done is rip someone else off for the price of a ticket that for some reason they never bothered to cancel. And stealing has always been relatively easy. You still would have to go through airport security so it's not like you've defeated anything on that end. It's been hammered into our heads that we need to be identified and checked at all stages of travel but there's nothing really convincing in that argument, nor does it have anything to do with security.

Dear *2600:*

Usually, when walking down an avenue in Brooklyn, New York, there aren't a lot of exciting or unusual things occurring. But today (8/21/09), I saw a black unmarked helicopter mounted with a large surveillance camera underneath the cockpit. I was walking on 5th Avenue and 45th Street in Brooklyn at 1:48 pm when I saw it flying low over the 4th Avenue area.

I know Sunset Park has cameras near intersections, but they are clearly marked with NYPD, whereas the helicopter I saw had no markings amongst the black paint. If it was NYPD, they need to mark this as such. If it was not NYPD, the public needs to be more informed about such matters. I could have snapped a few photos if I had been carrying my camera.

Jason

Which is precisely why people should always be carrying a camera. We have no choice but to assume you're making the whole thing up because you didn't have one.

Cries for Help

Dear *2600:*

I have a Sandisk Cruzer Micro-USB 2.0 flash drive from mid 2008. I need high level support for this situation, not assistance from amateurs. *Please* help or refer me to someone who can. I run Windows XP SP2 and created a password a few days ago for the flash drive. I didn't write it down and have now attempted to access it. The password is, I believe, nine characters and I know it for the most part. I tried a few attempts but after four it now says I have one left and if it too is wrong, the drive will lock permanently! I didn't realize I would be limited like that! I believe I would figure it out if I had a number of other attempts available.

I called Sandisk and they said I can select to redo the drive which will allow me to use the drive again but will erase all the data! This is not an option! I asked how I can 1) get a default password, 2) retrieve my password, 3) edit the drive to allow more password attempts, or 4) to retrieve the data. They responded that these things are not possible and that the information is encrypted (password info or my data?). I believe it is in fact possible!

Please tell me what all the options are. I would *greatly* appreciate your response for this matter as there is no other way really to replace all the files and I put a *lot* of effort and time into acquiring some and creating others!

Thank you *very* much!

Steve

There are allegedly companies that specialize in recovering such data but we can't vouch for them. We know a number of people are facing the same predicament as you but there are no immediate solutions. If there was any sort of hint question you used on setup, we suggest looking at that. We think the most promise lies in somehow defeating the limit on password attempts, if it can be determined how or where this is set. This is the flip side of implementing security: you may make things so secure that you lock yourself out. Of course, remembering a password really shouldn't be this big a deal in the first place. In the end, you may just wind up with a really valuable lesson out of all this.

Dear *2600:*

Recently, a couple of contributing editors from *2600* the magazine have been hacking my computer. I don't like it. I already have proof that one member has already hacked my computer. If people from your magazine continue to illegally hack my computer, I'll call the police. Please remove whatever backdoor your members have put on my computer.

I have hard evidence that I was hacked. I won't say who did it because I need this evi-

dence for a courtroom so I can have an advantage as the prosecutor.

anonymous

We think involving the cops is the best course of action at this point. We have an unmanageable staff and this is really the only way to get through to them. When the officers arrive, we'll be sure to have all of our staffpeople help them figure out what's really going on.

Best of luck in your career as a prosecutor.

Dear *2600:*

I don't think it's a writer of the magazine anymore that hacked me... however, the person is a member of *2600* in some way. I'd really prefer to avoid the police or a confrontation in that way. I did a whois on the domain and couldn't get an abuse email so I sent it here. It's that someone is hacking me and opening many windows on my machine and I want it to stop. They found out I had Knoppix on my computer....

anonymous (again)

No, it's OK really. Sometimes a head-on confrontation is the only way to deal with such matters. These people need to be taught a lesson, after all. Leaving windows open on a machine is an invitation to burglary and there's nothing funny about that. So we'll await the authorities and then lead them to the "member of 2600" that is making your life so miserable. Considering we don't actually have members, it shouldn't take long at all to get this resolved.

Dear *2600:*

I'm a key collector. Years ago, I purchased a huge lot of keys on eBay. I was after some other keys in the lot, however, there were some very interesting keys that caught my eye because I had never seen any like them before. So I kept them. I've recently learned these keys are older payphone keys. I've been able to identify most of them as "Western Electric." However, there are some keys I can't seem to identify the make of phone they belong to. Is there a chance you can help me to identify these other keys and maybe also confirm the others are in fact "Western Electric" as I've been told. I know these keys have some collector value and since they're not the type of keys I collect, I want to sell them to help recoup some of the money I spent on the lot and identifying the makers will help me with this. If this is something you can help me with, I can send you pictures of the keys. Please let me know and thanks for your time.

Jim

You're best off talking to people who collect either the old phones or some of the same types of keys. It might be good also to make sure it's legal to possess these keys. If it is, then going to various hacker or ham radio gatherings, or posting pictures online would be good ways to share information on this. You might want to consider asking the folks at Toool (The Open Organization of Lockpickers) who are easily findable on the net. If there's a chance these keys still work on existing payphones, you might not want to let too many people in on that.

Dear *2600:*

Hey guys, I was wondering if you can get the master key for a cell phone (Samsung Eternity) or maybe you can tell me where to find it. I found the admin settings, but no success on master key. Please help me.

josh

We're told that the master key setting is "#3971258*#" or "*#9072641*#" but that could be different for your particular model. The keys to input to get to the admin settings (which you already have) are allegedly "*#3695147*#." It's amazing how many people accept the premise that they're not allowed to have this information, even though it's for a phone they already own. Good luck in your endeavors.*

General Feedback

Dear *2600:*

As much as I want to believe there's something happening on the moon, what Etherni-um57 described in his 26:1 story (page 49) is a lens configuration issue and not, as he suggested, a clandestine moon base. I owned a telescope when I was a child and used to see the same kind of color distortions when I screwed my lenses together wrong.

The "rectangular beams" he describes, however, are quite anomalous. A call to *The Art Bell Show* might clarify that issue.

Gary

Dear *2600:*

I first wish to thank you for the variety of information that you impart in your magazine. *2600*, *Make*, and *Hakin9* are my three favorite magazines (in that descending order).

I just received my summer issue today and noticed the RENEW! notice on the envelope, so I immediately went online to renew. However, the only two choices I had for my "first issue" were Spring and Summer. I did not see a "renew" option. I will have to wait until that changes, I suppose, so I can have my first issue as the Autumn one and not get a dupe.

3lan

The software we use for our online store exists to make even the simplest things as frustrating and complicated as possible. But this actually isn't an example of that. What you mention is a feature we admittedly should have had from the start. In this case, since we don't keep our subscriber database anywhere near a net connection, it's not possible to access that information remotely. However, what we can do is add a feature that allows you to input your subscriber coding from your envelope and have us apply the renewal. Hopefully, by the time you read this, we will have that up and running.

Dear *2600:*

On the assumption that Dan's letter was not an exercise in sarcasm, I would like to point out a few problems with the approach of using a sentence as a password.

First of all, it is not "bulletproof against dictionary attacks." Despite the fact that there's more than one word in the sentence, all of the words are in a dictionary. Any good dictionary attack program has multiple-word attacks.

Second, while a sentence does make for a longer password, it doesn't necessarily make for a better one. As they say, it's not (just) the length that counts. An entire sentence can have less entropy (the degree to which one character is random compared to the other characters around it) than an eight character pseudo-random password.

Approaches like using the first letter of the words in a song lyric have the advantage that the password is easy to remember while still being pseudo-random.

yt

Dear *2600:*

I love the cover on the Summer 2009 issue. There are so many artifacts represented in it. I was looking for a photo credit and perhaps an indication of where and when it was taken.

The reference to the census, which takes places every decade, is at odds with the "Bicentennial Schedule."

Any info that can be shared would be appreciated.

Ed Greenberg

While finding out for sure is a bit difficult at the moment, it's not beyond the realm of possibility that the sign was simply lying around for a few years.

Dear *2600:*

What is the correlation to the two Emmas? Is that really the same tag that was shown on the baby's shirt in the last issue? Is the "real" operator Emma the grandmother?

Fiddles McHace

It's all in the history books. Or it will be.

Dear *2600:*

Every issue you go on and on about how hackers are portrayed wrongly and blamed for things they don't do. I think it is time you admit to yourselves that the word "hacker" has been redefined by society. It is just like how Frisbee started out as a brand of a flying disc and is now the de facto term for a flying disc; no amount of social pressure can change that. You are fighting a losing battle and no amount of education can turn this word back to what we want it to mean. By holding on to the word "hacker," you are only holding the hacker community back. It's time for a new term; how about a contest to come up with a new term for us? I'll start with the lame suggestion of "System Scientist"

tavis

You can make yet another term if you wish but you're going to face the exact same problems. People have tried to create words like "cracker" and "black hat" to define the more criminal elements in the hacker world. But all this does is give the mass media more words to demonize us with without adding anything constructive. We can, however, use the tarnishing of the word to our advantage if we're creative. After all, if you were to walk up to someone and admit that you were a "system scientist" or whatever phrase you come up with, we don't suspect their interest level would last much longer than wondering why you just walked up to them and said that. However, if you said you were a "hacker," you might see such reactions as panic, disgust, envy, or even hysterical laughter. In other words, you have their attention. Now, they may be filled with all sorts of misconceptions and factual inaccuracies and you may find yourself being bombarded with a number of them as a reaction to your proclamation. That is your opportunity to reach them and educate them with what you see as reality. If you do a good job, you will have dispelled a myth about what hackers stand for. Of course, the negative connotations will still be out there. But eventually, with enough people, those words will always be countered. We find it's better to stick around and fight for a belief, rather than retreat and concede something as important as a description of who you are. And you may be surprised by how many people already know that the mass media label is inaccurate. After all, in most movies and books, hackers are the good guys and the ones who eventually save the day, albeit through unconventional means. This can and should be a good thing.

Dear *2600:*

My wife has this obsession with prisonplanet.tv and infowars.com (the Alex Jones sites). And while some of his stuff makes total sense, I question most of it, including the flip side being our power hungry government! So I've had enough of the doom-n-gloom and decided to somehow kill those sites.

While my wife was away, I enabled Apache on her Mac, and modified her hosts file so that infowars.com and prisonplanet.tv resolved to localhost.

I found a cute small orange pirate skull and cross bones jpg and, through some html, had it repeat the image so no matter how she scaled the screen it was plastered in the entire browser window.

It then occurred to me: what if she punched me in the face, took my laptop, and hit those sites? Or what if she gets on her iPhone to check the sites? Our AT&T reception is horrible at home so she jumps on out wi-fi.

So I enabled "named" on her Mac and make sure our DHCP server handed out the DNS as her Mac. And I made sure that infowars and pris-

onplanet resolved to her Mac via some A record additions.

She got home, jumped on her Mac, and as she browsed those sites and said "Oh my God, see, the government hacked them!" I left the room, went outside, and laughed hysterically.

My advice to anyone wanting to do this: 1. Leave the room before your loved ones open the browser. 2. Put some duct tape over your mouth because my laugh was a dead giveaway.

Curious why in Ethernium57's article "Hacking: An Astronomer's Perspective," that while the entire article was awesome, the end was so abrupt and spoke about nonsense FaceBook garbage? I was waiting for what ended up being a wtf! I'm going to pull out my old Celestron and duct tape some lenses together now. Did you guys cover up his article in some way? Perhaps it's the secret base the elite will hide in during the 2012 planetwide catastrophe?

aurfalien

Dear *2600:*

In the future could you put up some more shirt designs that are more... subtle, like the seal one? Frankly, most of the designs are really not my style; they're too noisy.

S

Your vote for more subtle designs has been received. We're open to more suggestions as well. There are rumors of a new shirt in the works.

Dear *2600:*

I wanted to respond to the response from Sigma's article ("Exploiting Price-Matching through Javascript Injection," 26:1). Some deemed it unwise to print an article that gave explicit instructions on how to exploit a retailer and basically steal money out of its employees' pockets. I would say that as an employee at Best Buy, I was very grateful for that article. I was able to recreate Sigma's method and bring it to my manager's attention, thus allowing our business to be more aware of the possible exploitation of our policies.

Now, aside from the pat on the back I got for bringing this to the company's attention (thanks Sigma), I am grateful for the articles being published because part of hacking is finding these sources of exploitation, even if it means using some underhanded methods. It is really the only way to find out that there's a problem and make sure that it doesn't happen in the future. I'm even grateful that it was tested live in a store because that points out to the company that the management has grown lax in their overriding of price matches. This was not a complex method of theft; I could have done it when I was 12. But without having read that article, I wouldn't have thought of it. Thanks for the heads up, Sigma.

Clay

Dear *2600:*

This is my response to the rebuttal Michael gave to my article on "Social Engineering to Circumvent the Stock Market" (26:1). I'm sorry if I didn't explain who or what I am. I assumed that was a given. But I believe you missed the point of *2600 Magazine* and maybe the true meaning of hacking altogether. Maybe you took the legal disclaimer for granted. (I'll give you that one.) But I am not a thief, I'm a hacker. Telling a shopkeeper the lock on his door is broken is not a crime, nor ethically wrong. It is the thief who doesn't tell the shopkeeper their lock is broken who usually comes back and robs the place blind. You might question why I chose to have this published in a hacking magazine versus just, say, calling Wall Street or the oil companies myself. That is because those kinds of calls usually fall on deaf ears. (Thus, "gray hat hacking" was born.) Meanwhile, the system is flawed and open to attack. It is only a matter of time before someone comes along who doesn't tell the shopkeeper the lock is broken. If people do not know an attack is coming, they are a victim. But if they were warned an attack is coming that could've been prevented and they do nothing about it to fix it, they're just stupid. I believe we should educate the public and at least give them a chance.

I did find it humorous that you really think that the oil market jumping so high in 2008 was all due to demand. True, there are now more people driving in China, but the Soviet Union's devolution opened up a vast supply of oil which, according to rules of supply and demand, should have dropped the price by flooding the market. But it never did, even before China accepted state capitalism where their driving community took off. Even now, if you keep up on the news, the big oil companies have shut down more and more supply lines of oil for no other reason than the price has dropped. Even at $3.50 a gallon, they admittedly started doing this to try and drive it back up. You said I should have researched this more. I now challenge you to do the same.

If the projects you're referring to in Alberta, Canada are what I think they are, I really don't care. I assume you're talking about that project to force underground compression to create oil that would normally take Mother Nature lifetimes. It was only viable if oil prices were high, otherwise production would not meet demand. I really don't care if your country or my country or whoever becomes the next oil kingpins. There are solutions out there for us to use alternative energy in vehicles that are not only cheaper and cleaner, but faster and better built. I suggest you watch the movie *Who Killed The Electric Car?*

Oh yeah, read the real definition of a "hacker" and "cracker" sometime and stop demonizing people you do not understand.

P.S. *2600,* I love you guys but you got to learn to spell my name right. It's Israel, not Isreal.

Israel

Your name was spelled that way because that's how you spelled it in your initial article submission. Until you told us otherwise, we had to assume that was how you wanted it spelled and so any reference to your article by other let-

ter writers had the proper spelling "corrected" to the one you gave us. Not a whole lot we could do about that.

Dear *2600:*

In 26:2, Michael asked what the acronym HTH stood for and it was (most likely) incorrectly answered with "helix-turn-helix." I believe HTH in that context (signed at the end of a message) almost certainly stood for "Happy To Help" or "Hope This Helps." The acronym HTH being used for this meaning has become a common occurrence on the large SomethingAwful forums, which is probably where the message writer got it from.

HTH
Ryau

It's amazing how we somehow managed to miss that, even while signing our own response to the question of what HTH meant with "hope this helps." It just goes to show that our readers don't ever miss a trick. Mostly.

Dear *2600:*

I cannot thank you enough, KES, for your article "Simple how-to on Wireless and Windows Cracking" in 26:2. Your guide was so easy to follow that I was able to crack a WEP key the very first time I tried with no problems. The only thing I did differently was install the Aircrack-ng suite on my laptop already running Ubuntu 9.04 instead of using the BackTrack distro. I have always wanted to try this but was never really successful. I did notice one small error. In the command where you run airodump-ng, it says "-bssid" but that gave me an error and told me to use "--bssid" instead. After I changed it, it worked like a champ. You also opened my eyes about how insecure WEP really is, so I'm changing my own router to WPA. Thanks again for making this so easy. Happy Hacking!

Justin

Dear *2600:*

I subscribe and I just read the privacy article by 6-Pack (26:2). Fantastic and *very helpful*. How do I send him or her a snail mail letter? If I send it to you with extra postage, can you forward it? I would never ask you to give out an address, so I must ask your help on this matter. I have a few other questions and I would like to send this person a *free* copy of a book I wrote. It is the reason why this article is so important to me. My book is titled: *James Earl Ray - The Last Days of Inmate # 65477* and I receive death threats every now and then and I have a persistent stalker as well.

I would like to send you a copy too. Do I use the Middle Island, NY address on the back of your cover?

Michael Gabriel

You can send us anything at our address. If the writer requests us to forward something reasonable, we will do that as well.

Dear *2600:*

To 6-Pack: You don't have to apologize for using the street address of the post office. There is a provision in the U.S. Post Office DMM (Domestic Mail Manual) which provides that one can use a street address plus a box address and that the mail is to be delivered to the address that is immediately above the city and the state.

The DMM provision does *not* prohibit the use of the street address of the post office; it is like any other street address! Therefore, one can *legally* and properly use the street address of the post office, then the box number you are using, and then the city/state. The DMM is online and you can look up the exact provision for dual address delivery. Further, *even if* the address is wrong, *if* the post office employee knows the correct address for delivery, that employee *must* deliver it to the recipient - regardless of a wrong address on the mail!

The post office *must* deliver the mail to the box number regardless of whatever street address is indicated above the box number. In fact, one could probably use a phony street address and then a legitimate box number and the mail *must* be delivered to the box number. Those recording addresses will then pick up the phony street address, hopefully!

Also of interest, temporary forwarding addresses are not available to marketing companies, only permanent changes of address with the post office. Therefore, one is wise if moving and not wanting the new address to be part of the public record, they put in a "temporary" address for 11 months. Then, after the 11 months, one can then submit another "temporary" address for another 11 months. It works well.

Enjoyed your article - well done and thought out. I have been protecting my privacy for years!

Always pay your cable, telephone bill, electric, water, etc. with a money order. These companies *record* the source of your payments. They have your checking account number, bank, etc. Therefore, pay them with a non-traceable payment. *Don't ever* use your credit card, *don't ever* use a credit card, *don't ever* allow "automatic pay" since it is not only recorded, but hard to contest later.

Pay in advance if you must, but be careful *how* and in *what manner* you pay these utilities. Your *privacy is at stake!*

Fiducia

Let's see how many people can send us a secret message in the line before our PO box or simply enter a really funny street address that will never get used. Of course, just because something is supposed to work in a certain way in the post office is no guarantee that it will. But just for the fun of it, let's try. Send your next postal letter to: 2600 Letters, [insert wacky message or one-line address here], PO Box 99, Middle Island, NY 11953. Be sure to have your return address on the envelope in case you break something in the system.

HARD DISK ENCRYPTION, NO EXCUSES

by GhostRydr

In today's society, with laptops and portable devices easily available and easily stolen, hard disk encryption is no longer optional. This should be something that everyone with a laptop has installed. For most people, there is a lot more personally identifiable information on your laptop than one might think. Information that is not even stored on your laptop, but is accessed through websites that require a login, is easily accessible to any common thug if you save your login information in your browser. If you use Windows and think your Windows password will save you, think again. Using a Trinity Rescue Kit CD, a Windows password can be hacked in less then five minutes. Almost every day, it seems we are hearing about another staggering amount of customer information that was lost and compromised due to a laptop theft that could have been prevented by the simple use of disk encryption. While losing your laptop sucks, and will cost you several hundred dollars, having your identity stolen really sucks and can cost you even more.

At my work, I was recently handed the project of devising a solution to encrypt the hard disks of all our portable users. Since being introduced to *2600* a few years ago by a close friend, I've become very interested in security and related matters, so you can imagine how thrilled I was when this project was handed to me. I started out not knowing much about hard disk encryption, but this changed very quickly. My research took me down several different paths and, interfacing with different software vendors, eventually lead me to choose PGP's Whole Disk Encryption. Their corporate products are very good and they also offer a personal version for $120. However, I'd like to focus on another piece of software called Truecrypt.

Truecrypt is a 100% free, open source disk encryption application from `http://www.truecrypt.org/`. It is easy to use and is capable of encrypting your entire hard disk from start to finish using several standardized encryption algorithms including AES, Serpent, and Twofish. It essentially wraps each block of data on your hard drive using an encryption algorithm which is virtually unbreakable. The only real change you will see is a pre-boot environment that will appear after the BIOS screen, asking you to key in your password and unlock the disk. Once this is done, your computer will boot as normal. I know some of you will say that hard disk encryption really kills your system's performance. Contrary to that, system performance is almost unaffected. Some users even report a slight increase in performance, due to a pipelining effect that happens to the read and write operations. Truecrypt stores the encryption keys in RAM and decrypts the data on the fly. Data is unencrypted as it comes off the disk and then encrypted again before it ever touches the disk. And best of all, its free! The complete source code is available for download from `http://www.truecrypt.org/downloads2.php`, which means no worries of hidden back doors for Big Brother. The install is very simple and, once your drive is encrypted, your data is safe from almost any attack method.

To begin, download the installer from `http://www.truecrypt.org/downloads.php`, choose your flavor of operating system, Microsoft, Linux, or OS X, then download and install the package. The website has complete documentation on many other features, including portable USB drive encryption, but for this article I will just show you how easy it is to encrypt your hard disk. After installing, launch Truecrypt, select the "edit" menu, and then select "encrypt system partition/ drive." At the first screen, you can choose a "normal" or "hidden" encrypted partition, the difference being that a hidden encrypted partition, simply put, will be indistinguishable from random data. An extra layer of protection, if you think you need it. For now let's go with "normal." Next, you can choose to either encrypt just the Windows boot partition or the entire physical disk. Choose the entire disk if you have 2 or more partitions and want to encrypt everything. Next, choose whether you want to encrypt the host protected area. Depending on your computer setup, select the option you think will work best. At the next screen choose whether or not you have multiple operating systems installed and move forward.

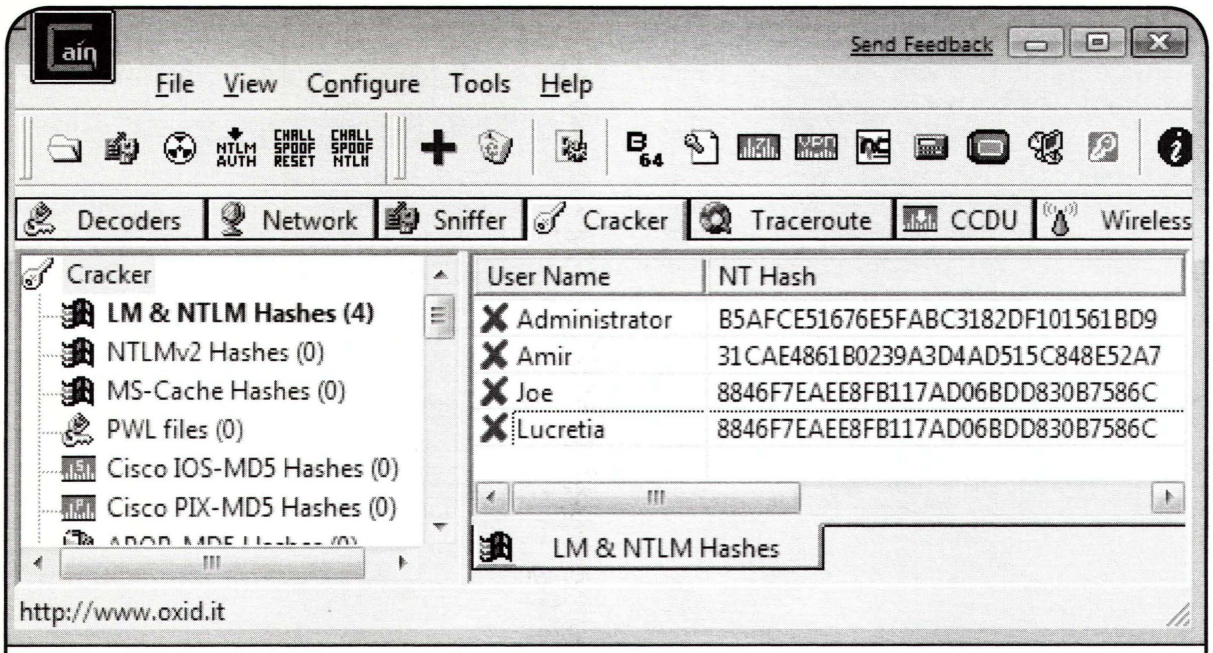
Now you should be at the Encryption Options window. This is where you can choose which algorithm(s) you want to use. AES is the default and is very secure. However, if you're feeling paranoid, Truecrypt will allow you to use up to three different algorithms together, essentially wrapping each block of data with three different layers of encryption. Keep in mind, the more layers you use, the higher the impact on system performance. Using one layer should be sufficient for most. For the Hash Algorithm, RIPEMD-160 (default) will do. Next, choose a password that you will use to unlock

the disk before the operating system loads. The software will recommend using a 20 character password, which is not necessary, but be sure to use common sense when choosing a password. At the next prompt, move your mouse around to help randomize the encryption keys. Click next to see the encryption keys and then move on to create a rescue CD. Truecrypt will not allow you to continue without creating a rescue CD. If the Truecrypt boot loader ever gets damaged after you have encrypted your disk, it can be restored using the CD. Once you've burned the rescue CD and verified it with Truecrypt, click next. Select which level of "wipe mode" you prefer. The default "none" will be suitable for most, but depending on how sensitive the information you store on your laptop is, you may want to choose a more secure method. To test the system before it encrypts the disk, Truecrypt will reboot your system to ensure everything works correctly with the pre-boot authentication. Upon reboot, key in the password you specified during setup and boot into your OS. At this point, the test will complete and the encryption process will begin.

The time it takes to fully encrypt your hard disk will depend on the size of your disk and the system specs. A 40GB drive on a Pentium 4, 3GHz, was about 35 minutes. Once this is complete, your data will be secured and your entire hard disk will be encrypted. Remember that no single security method is 100% secure and security is best applied in layers. With that in mind, laptop anti-theft devices are still a good idea, including cable locks, tracking software, and even laptop lockers.

Shouts to Rob for getting me hooked on 2600 and making this possible! See you back on The Rock!

◇◇◇



that from the salted hashes. Attackers can't make a dictionary of password hashes now, unless they make thousands of dictionaries, one for each possible salt value.

How does Windows store passwords?

To find out, I made the accounts shown above on a Windows 7 Beta machine. Then I used the free program "Cain" from oxid.it/cain.html to dump the hashes. To do that, just click on the "Cracker" tab, right-click the center of the window, and click "Add to list". Then click "Next". As you can see in Figure One, the hashed values are the same for "Joe" and "Lucretia". I tested this on Windows 7 Beta (32-bit), Windows Vista Business (32-bit), Windows XP Professional (32-bit), and Windows 2000 Professional, and the hash for "password" was identical in all cases. I also confirmed that the hash is the same for a local account on a Windows 2008 Server Datacenter 64-bit machine, using fgdump (from `http://swamp.foofus.net/`) to gather the hashes.

Conclusion

The statement in the "Hacking Exposed" book is correct: Windows does not salt its password hashes. This is a shameful security error on Microsoft's part, and needs to be corrected. The Unix "crypt" man page says this feature has been included in Unix since versions 6 & 7 of AT&T Unix, which came out in 1975 and 1979. How can Microsoft continue to use a system which has been obsolete for 30 years? We, the consumers, need to demand more. I hope that this article may help to shame Microsoft into doing better work.

About the author

Sam Bowne teaches Ethical Hacking and other classes in the Computer Networking and Information Technology department at City College San Francisco. His website is `http://samsclass.info/`.

Table Three: Salting and Hashing Passwords

Username	Password	Salt	Password+Salt	Hashed Password+Salt
Administrator	zaphod	WM	zaphodWM	759e9786a86814820d19a8d4b642443a
Amir	opensesame	45	opensesame45	c559d397235a44bf906d4f86cdd3e1a9
Joe	password	q2	passwordq2	984e1b8949abbd846399e38d0f2cae81
Lucretia	password	2r	password2r	55d1776bb284bbba75ddb31e3480b000

Table Four: Salted and Hashed Password Storage

Username	Salt:Salted Password Hash
Administrator	WM:759e9786a86814820d19a8d4b642443a
Amir	45:c559d397235a44bf906d4f86cdd3e1a9
Joe	q2:984e1b8949abbd846399e38d0f2cae81
Lucretia	2r:55d1776bb284bbba75ddb31e3480b000

Amazing Grace Period:
How To Get Free Loans From American Express

by Bavs

Just like any red-blooded American, my wallet is bursting with credit cards from various banks that are more than happy to give me huge amounts of purchasing power in exchange for exorbitant APRs.

My personal favorites are my American Express cards, as they give me tons of frequent flyer miles and come with an almost three week grace period each month to pay my bill.

The following is a way to exploit this grace period, to help keep your account in good standing and avoid accruing interest charges.

Step 1: Determine how short you are for the month

As soon as your account closes for the month at hand, check your balance online and do some quick arithmetic to determine if you'll have enough cash by the due date to pay in full. If not, take note of how short you are and mosey on over to your local mall. Don't forget your credit card.

Step 2: Buy something

Walk into a store with a good return policy and charge something that costs at least the amount of money that you are short to the same card.

Step 3: Return it

Make sure that you have the cashier credit your card. This step must be done with sufficient time left to allow for the return credit to hit your account before the grace period ends.

Step 4: Wait for the credit to post

Now here's the cool part. The purchase that you made will be included in the next billing cycle but, if you check the outstanding balance for your current bill, you will see that it has decreased by the amount of the return as Amex applies the credit to your account immediately, creating a mismatch between payment cycles!

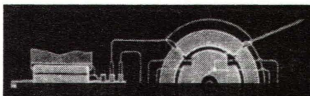
Step 5: Pay your bill "in full"

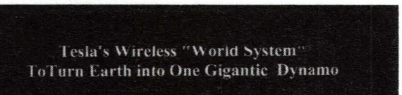
Keep in mind, though, that this trick will not give you a free pass on the return money. You will have to repay it in full the next month, but you have successfully received a free loan from American Express and avoided accruing any interest fees! Keep that credit crisis rolling!

Shout-outs: Galaxy and The Coot

The Next HOPE

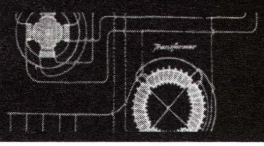
July 16-18, 2010
Hotel Pennsylvania
New York City
U.S.A.
www.hope.net

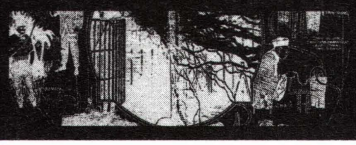




Transmissions

by Dragorn





Lean back and remember the 1980s (if you can), or complain about old people always talking about "the good old days" if you can't (and while you're at it, get off my damn lawn with your rap music and your skateboards). Imagine... a cheesy flashback ripple effect... Think back... Back to the days of big hair, ripped jeans, GI Joe being just a cartoon, synthesizers, and shared media networks.

Shared media networks - the predecessors of modern switched networks - were a hacker's playground. Instead of virtual circuits between the systems communicating, every system on the network got the packets from every other system. Anything anyone else on your segment did was visible, and anything you did could affect all other users on the network.

Too bad the good (which is to say, bad) old days are long gone, right? We'll never see their like again. Everything now is switched, protected, encrypted. I'll just take my laptop and go sulk at the coffee shop and leech a little free wi-fi. Free, unencrypted wi-fi. Where all the users are on the same channel. Sharing the same network. On a shared physical medium. That's right, wi-fi is a time machine to the 80s. All the old tricks work, we just need to tweak them around a bit.

Most likely the best trick that most of us have forgotten all about is TCP session hijacking. TCP is only "secure" (that is, secure from being spoofed from random attackers) in so much as it uses a random sequence number. The sequence number is used to ensure that all packets are delivered, that the packets are delivered in order, and that the packets came from a host which knows the proper sequence. Without this sequence number, packets which claim to be part of a connection are discarded. On a shared network like open wi-fi, this number is by no means random or unknown.

Performing a TCP hijack is the same as it's ever been: Capture packets, extract the sequence number, and reply quicker than the foreign system. Every TCP connection goes through a handshake stage where the client and server exchange sequence numbers and establish the connection, and packets sent from then on advance the sequence number by the number of bytes sent.

Sessions can be hijacked at the beginning of the connection by spoofing the remote system during the handshake process, but they can also be hijacked in the middle of a stream by beating the next legitimate packet. A local attacker is closer, and therefore able to respond more quickly than a remote host which can be thousands of miles and many routers away, each hop taking more time to navigate. Exploiting this allows matching things like HTTP requests and replacing them. In fact, exactly this attack was shown about five years ago at DefCon in Airpwn by Toast... and then promptly forgotten as anything other than a method to make people look at goatse.

The obvious risk from this (and one many attendees of DefCon learned to their dismay) is replacement of any web content with any other arbitrary content. Unfortunately, this is by no means limited to simply pranking. When a TCP session is spoofed, it is indistinguishable from traffic coming from the legitimate host. Arguably, timing might reveal that the packets are coming from a closer source than a physically distant remote host, but for all practical purposes a client application will have no chance of detecting a spoof attack. The HTTP security model is generally based around the idea that only javascript code which is part of a page, or which is included by a page, is allowed to alter the page. Cookies are based on domain controls so that only websites which appear to be the proper domain can access them. Browsers such as Chrome segregate individual pages into separate instances to prevent cross-contamination.

All of these protections are eliminated when surfing an unencrypted website on an open network. Most modern AJAX-ified Web Two Point Whatever pages include helper javascript (and often, dozens of helper javascript) files when they load. Any one of those javascript helper files has privileges to control

the content of the website. By delaying the TCP session hijack until the handshake is completed and the user has requested a file, it becomes easy to target specific files (for example, a tracking/statistics file from a popular company which rhymes with "moogle").

So, someone has fed you a poisoned javascript file. What can happen to you? Just about anything. Having your browser fed a selection of the latest exploits is one obvious result, but once inside the DOM it becomes trivial to rewrite the content of pages on the fly, opening a variety of possibilities.

For example, replacing every https link with the unencrypted http equivalent:

```
var refs = document.
➥getElementsByTagName('a');
for (var i = 0; i < refs.length;
➥i++) {
   var rval = refs[i].
➥getAttribute("href");
   if (rval == null) { continue; }
   refs[i].setAttribute("href",
➥rval.replace(/^https:/, "http:");
}
```

Once inside the DOM, redirecting forms, poisoning links, extracting cookies, and loading additional attacks becomes a trivial, but major, risk.

The chances of picking up something unpleasant from public networks is compounded when you consider the risks of the browser cache. Files loaded in the background are just as cacheable as normal web pages. Think about that one again, slowly. Javascript helper files, which we just saw being altered for fun and profit, can be set to cache. Once cached, a hostile file will remain until the browser cache is cleared, the cache expires, or the page using it changes to include another file. Detailed by Robert Hansen at `http://www.sectheory.com/➥rfc1918-security-issues.htm`, controlling the cache of a page on an insecure network can lead to control of secure content later.

The cache is controlled by the HTTP headers. The HTTP headers are, of course, returned as part of the TCP stream. When the TCP stream can no longer be trusted, no content can be considered safe. Even websites which normally are not considered trusted, because they don't require a login, or aren't something you care about (if, for some inexplicable reason, you don't mind someone having one of your logins somewhere), may now lurk, waiting for an opportunity later.

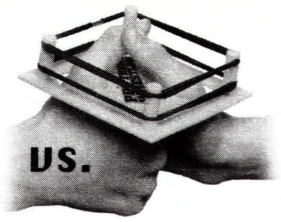
Once in your cache, a hostile file can call home each time it's loaded. This might be when you're at home, or at the office. The spiked file may do nothing for a month, acting completely normally, until a new browser vulnerability allows a takeover of the whole system. Even without exploiting the browser, purely browser-level issues such as wrapping all future browsing in an iframe can still compromise sessions.

These risks are inherent in any open network, and avoiding them is very difficult. The only way to avoid bringing home something unexpected from the coffee shop wi-fi is pretty much the same as the precautions you should be taking already, with one notable addition: Use a VPN or SSH tunnel for all traffic. The addition? Use it for *all* traffic. Even "low-trust" web pages remaining in your cache indefinitely until the next browser 0-day hits and they include a new attack via a cached callback. Simply clearing the cache or setting the browser to not cache may prevent retaining poisoned content, but that won't prevent local attacks from working in the first place.

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

SSL  DNSSEC

by John Bayne
stephan@scandinode.com

DNSSEC is a promising technology that will increase trust on the Internet. DNSSEC stands for Domain Name System Security Extension and adds security to domain name lookups. DNSSEC enables you to identify sites on the Internet so that you really know that you are communicating with the correct one. The technology came into the spotlight during 2008 because of two events:

1. Dan Kaminsky[1]. You have some serious reading to do if you don't know who that is.
2. The US Federal government announced that they would sign the .gov top level domain. The Office of Management and Budget (OMB) issued a memorandum requiring agencies under .gov to sign their domains[2].

TLS, that more popularly is being referred to as SSL, works by installing a digital certificate on the web server, allowing users to connect via secure HTTPS instead of HTTP. We have all seen HTTPS in action and most readers probably have a general knowledge of how it works.

Some people think that DNSSEC will save the world and that everything will be safe after implementing DNSSEC. Some think that it will prevent spam and guarantee that senders aren't forged. Some even think that it will stop phishing attacks. I think that DNSSEC is a nice addition that complements existing technologies.

For one particular problem, DNSSEC and SSL overlap. Both DNSSEC and SSL are designed with integrity as a goal. That is, how certain we are that the site we are visiting actually is the one it claims to be. As both technologies solve the same problem, one can question if we need to use them both?

- Can I turn SSL off if I'm using DNSSEC?
- Do I really have to implement DNSSEC if I already have SSL?

This article is a seven-round match up between the two technologies. I will analyze which integrity mechanisms the technologies can provide, how they are implemented, and how they differ.

Just to be clear, both technologies provide additional security benefits that are not covered in this article. The technologies will never be mutually exclusive. For example, SSL can encrypt data to guarantee confidentiality. DNSSEC allows for authenticated denial of existence (very useful?).

Round 1: Trust

How is trust implemented in each technology?

Both technologies provides endpoint authentication of the server you are communicating with. The authentication stems from the fact that there is a chain of trust that you can follow to verify the identity. Both technologies have higher authorities that vouch for an identity. In SSL this higher authority is the issuer of the certificate. Those higher authorities are listed in your browser.

In DNSSEC, you normally specify the higher authorities with trust-anchors in your resolving DNS. It is very likely that DNS software will come preconfigured with trust anchors in the future, much like browsers come preconfigured with a list of certificate authorities to trust.

Security is never stronger than its weakest link. We must therefore analyze the process of how the public key gets signed and how the certificate is obtained to be able to score this round. In DNSSEC there is no certificate sent back to the requester, instead trust is established by special DNS records that are published and signed by the top level domain. The end result, however, is the same.

In SSL, the certificate issuer is supposed to check the identity of the requester before a certificate is issued. In DNSSEC, the parent domain (typically the top level domain) should check the identity of the child before the records are signed and published. Not that much of a difference between the technologies there, either.

Recently, a security researcher, Eddy Nidd, managed to get an SSL certificate for a domain that he wasn't affiliated with[3]. His little experiment exposed a weakness in the SSL certificate issuing process. The issuer did not authenticate the requester correctly. The experiment undermined the trust of SSL certificates in general. As we no longer can trust that the certificate issuers are doing their jobs correctly, we can no longer trust SSL certificates in general.

DNSSEC will face the same control and regulation challenges as SSL certificates do. Each top level domain (such as .SE, .ORG, .MIL, .UK) needs to have an authentication process in place to make sure that only valid requests get signed and published. So far, there is no central policy on how the authentication must

be performed and there are no control mechanisms in place to control the top level domains. Some top level domains (yes, you guessed it) use SSL to secure communication when users are being authenticated.

There are about the same number of certificate issuers in a browser as there are top level domains, so implementing controls will face the same type of challenges in both technologies. In fact, the challenges are even worse in DNSSEC as most top level domains use third party registration partners to do the actual authentication of the requester. There are thousands of third party registration partners that have to authenticate the requester in a secure way.

How do we make sure that every top level domain and every registrar implements the controls correctly? We can't, and therefore the trust in DNSSEC can be questioned.

SSL has some obvious flaws when it comes to authenticating the requester of the certificate. There is no central body that oversees and audits the certificate authorities. On the other hand, DNSSEC suffers from the same dilemma, and there is no way of knowing that the DNS community would do a better job.

This round is a draw; both technologies lack control mechanisms for how trust is implemented.

Round 2: Algorithms

How strong are the algorithms that are in use?

In the beginning of 2009, Alexander Sotirov found an issue with SSL allowing him to create a rogue Certification Authority (CA) certificate trusted by all common web browsers[4]. This certificate allows us to impersonate any website on the Internet. He took advantage of the weak MD5 security algorithm that is in widespread use in SSL certificates. In fact, one certificate out of seven is using this old and deprecated MD5 security algorithm[5]. The SSL community should have ditched MD5 a long time ago. The Certificate Authority in question was RapidSSL, owned by Verisign. Tim Callan of Verisign quickly wrote an article in Securityfocus claiming that "MD5 Hack Interesting, But Not Threatening"[6]. What he forgot to explain is that there might be one or more fake Certificate Authorities out there that can issue valid certificates for any server. (If you ever feel that you would like to stop trusting a particular CA, you can do so by going to Tools/Options/Advanced/View certificates/Delete in Firefox)

The MD5 algorithm is deprecated in DNSSEC. Therefore, DNSSEC is the winner in this round.

Round 3: End to end

Does the technology provide true end to end security?

SSL provides near end to end security, as the traffic is secured between the browser and the web server. The only way to interfere with SSL would be at the end nodes. SSL is implemented on top of the communication protocol it is securing. It is therefore impossible to tamper with the communication, even if you have access to a computer or router in its path.

DNSSEC is not end to end. It is typically only secure between the resolving DNS server and the authoritative DNS server and not all the way up to the client. We need to wait for full DNSSEC support from the client operating system before we can have a true end to end security. The next version of Windows will only ship with a "non-validating, security-aware stub resolver." These types of resolvers are not true end to end[7]. Instead, the resolving DNS server at the client side validates the records and notifies the client about the outcome.

The lack of end to end security makes DNSSEC vulnerable for attacks in the last hop between the resolving DNS server and the client. An attacker could potentially tamper with the packets between the resolving DNS and the client to trick the client into thinking that the digital signature of the requested resource record is valid. The RFC recommends that IPSEC be used as a mechanism to prevent this. That would, however, be hard to implement and maintain in a real world environment. It is yet to be seen how DNSSEC will handle this.

DNSSEC only secures the DNS lookup, and not the communication. To make an analogy, you are securing the phone book lookup but not the actual call. Somebody with access to a computer in the path between the sender and receiver can potentially tamper with communication.

The true end to end capabilities of SSL makes it a winner in this round.

Round 4: User Warnings

How clear is the warning that the technology present to the user about invalid certificates/resource records?

SSL is often criticized for the visual warnings (or lack thereof) that are presented to the user. The visual warning is determined by how it is implemented in the browser. The warnings usually consist of a small padlock icon, or a green background in the address field. Although the warnings have become better and clearer with the newer versions of browsers, they are still not up to the challenge. Most users don't check to make sure that they are on a secure site when they are, for example, doing online

banking.

DNSSEC faces the same issues with user warnings and has yet to prove if it is up to the challenge. There is very little client side support in operating systems and browsers for DNSSEC, and the few implementations that are out there don't look very different from what SSL is providing[8].

Even with the identified problems with SSL, it still wins this round. DNSSEC has a chance to catch up in this category if they implement a better warning system.

Round 5: Centralized configuration

How easy is it to implement a centralized policy for the technology?

To be able to centrally configure a policy on what is allowed, instead of relying on users, is obviously a huge advantage on any network. Most people argue that one of the biggest challenges for SSL is the fact that the user can override and continue to a site even if a certificate is invalid (for example, expired or issued to another host). Perhaps less known is that this can be blocked at the network layer in a proxy or similar device. Some proxy servers can be set up in such way that a centralized certificate policy is enforced. For example, a proxy server can be set up in such way that it disallows users to continue if the certificate is invalid.

In DNSSEC, you have a resolving DNS server between the client and the site that you are communicating with. The resolving DNS server is typically where you configure the trust anchors and where the validations of signatures occur. The client will be prevented from continuing if the validation fails, as the associated bogus records will not be sent back. However, this behavior can be circumvented by the client by setting the checking disabled (CD) bit in the query[9]. This will force the resolving DNS server to respond, even when the signature doesn't validate. This behavior is a requirement in the RFC, so there is not that much we can do about it. There is really no good way to implement a centralized configuration in DNSSEC.

SSL can be configured with a central policy, DNSSEC can't. SSL wins this round.

Round 6: Adoption

How widespread is the technology?

SSL has been around for many years and is a technology that is much more widespread in use than DNSSEC. There is extensive support for SSL in both browsers and servers.

DNSSEC has a shorter history and is not widely adopted. The technology has suffered from the chicken and the egg dilemma. As no zones were signed, it didn't make sense to implement DNSSEC on the client side and, as clients never checked the signatures, it didn't make sense for domain owners to sign their domains. Furthermore, just a few top level domains support DNSSEC so, for the vast majority, it is next to impossible to implement DNSSEC even if they wanted to. The egg is about to crack with initiatives such as the OMB mandate, but it will take several years before DNSSEC will be adopted in such scale that it will be usable for any real life scenarios. Right now, DNSSEC can only add security in the rare cases when you know that both endpoints support the technology, such as for internal communication or communication with a partner.

SSL is the clear winner in this round; DNSSSEC has a lot of catching up to do.

Round 7: Scope

How broadly will the technology protect you?

A security technology should have a broad scope, to be able to provide protection for many different servers and applications.

Although it is possible to purchase a wildcard SSL certificate that can be used on any server in your domain, it is more common to purchase individual certificates per server. Usually only external facing web servers gets the privilege of having a real SSL certificate. Each application needs to be secured individually and there is typically a secured counterpart to each insecure application (FTP vs. FTPS, HTTP vs. HTTPS, LDAP vs. LDAPS). The scope of SSL is normally limited to one application on one server.

DNSSEC is implemented on a per zone basis. Signing additional resource records can be done with little extra effort. This makes DNSSEC a winner in this round.

Summary

Both DNSSEC and SSL aim at solving the integrity problem and both are doing a pretty good job. Time has proven that SSL is a usable and reliable technology. DNSSEC is a promising technology, but is much less mature. SSL wins four rounds, DNSSEC wins two, and one is a draw. DNSSEC has the possibility to catch up. As DNSSEC gets implemented on a broader scale, we will see if the technology is up to the challenge.

Back to the questions

Can I turn SSL off if I'm using DNSSEC?

No, even if encryption is solved by some other means, I would strongly advise against turning off SSL just because you implemented DNSSEC. DNSSEC doesn't really protect communication, just DNS lookups, and DNSSEC is not truly end to end. SSL is here to stay.

Do I really have to implement DNSSEC if I already have SSL?

If you are only looking to secure one server and one application and you already have SSL, there is not much to be gained by implementing DNSSEC. SSL is designed to provide the required protection by itself. But if you are looking at security from a broader perspective, you would probably want to add DNSSEC. DNSSEC has a broad scope and it is easy to add security all your servers and applications with little extra effort. Of course, the best thing is always to implement both technologies.

To sum it up: Both DNSSEC and SSL are needed.

References

1) Dan Kaminsky, US cert advisory, http://www.us-cert.gov/cas/techalerts/TA08-190B.html

2) OMB DNSSEC mandate, http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf

3) Eddy Nidd SSL certificate hijack, https://blog.startcom.org/?p=145

4) Alexander Sotirov rough CA, http://www.phreedom.org/research/rogue-ca/

5) Use of MD5 in SSL, http://news.netcraft.com/archives/2009/01/01/14_of_ssl_certificates_signed_using_vulnerable_md5_algorithm.html

6) Tim Callan Securityfocus, http://www.securityfocus.com/columnists/488

7) DNSSEC in Windows 7, http://blogs.technet.com/sseshad/archive/2008/10/30/dnssec-in-windows-7.aspx

8) Drill extension to Firefox, http://www.nlnetlabs.nl/projects/drill/drill_extension.html

9) RFC 4035, the CD bit, Section 3.2.2 http://www.rfc-archive.org/getrfc.php?rfc=4035

Tethering the Samsung SCH-R450 on MetroPCS

by VXO

Introduction

MetroPCS is a flat-rate CDMA wireless carrier with service in some larger metropolitan areas throughout the United States. MetroPCS service requires no contract, and uses customer-owned handsets. The service plans include unlimited use of local and long distance voice services. Text messaging, picture messaging, voicemail, and wireless web access are available on higher plan levels, or are available seperately. The plans range from $30 to $50 per month.

The phones available on MetroPCS currently range from the more basic "candybar" handset at $80 to a Blackberry Curve at $450. Various MetroPCS phones are plentiful on eBay and other sources.

The Samsung SCH-R450

Before the Blackberry Curve was offered, the R450 Messager was MetroPCS's only offering with a full keyboard.

The top of the phone slides sideways, exposing the full QWERTY keyboard below. The display will flip to landscape when you turn the phone. Strangely, the BREW environment and browser only operate with the slide open. The BREW implementation on the older Kyocera Strobe would operate on the external or internal LCDs.

The R450 has a 1xRTT connection, BREW software environment, 1280x960 pixel camera, Bluetooth audio and object exchange profiles, GPS, MicroSD socket, music player, and built-in Openwave web browser.

BREW applications available for the phone include Metro411 (a V-Enable Mobile411 directory assistance app), Mail@Metro (an e-mail client), Loopt, and a Mobile IM client.

BitPIM does not recognize the phone yet. It doesn't appear to support the proper AT commands to kick it into BREW mode, and won't talk to it as "Generic CDMA phone" or anything. To get files on and off of the phone, use USB storage or Bluetooth object exchange.

External sockets are provided for a mono or stereo headset with 2.5mm plug, and a port for a USB data cable, charger, or other compatible accessories.

The USB cable is provided in the box. No accompanying software is supplied. In the menu under Settings / Phone Settings / PC Connection, you can enable or disable USB mass storage. If you have USB storage enabled, plugging in the phone will put it into USB mass storage mode. Nothing else functions while it's in USB storage mode, though the phone will charge. When you're done, unmount the volume and press the soft key for "Done" to go back to normal operation.

The phone will charge on any powered USB 1 or 2 port. No driver is required for charging.

This handset is not nerfed like the Razr!

USB CDC ACM class modem support is present on the phone, but it's disabled out of the box. Once this is enabled, if you have the wireless web feature enabled on your account, you can hook the phone up to your computer and use it as a wireless data connection.

Press OK to get into the menu, then 9 #. The phone will ask for a code, which is 587846. You'll see a number of otherwise hidden options, including DUN mode. Scroll down to DUN mode and turn it on, then power cycle the phone, just for good luck and fortune. Connect the USB cable and you should get a USB CDC ACM class modem device!

On Linux, this will be /dev/ttyACM0. On Mac OS X 10.5, it will show up as /dev/tty.usbmodem***. On 10.4 it comes up as something different. ls /dev | grep -i modem should show it. The output of dmesg should show something like this:

AppleUSBCDCACMData: Version number - 3.1.9, Input buffers 8, Output buffers 16

If you use ZTerm or minicom to connect to the serial device, you should be able to get the usual modem responses. AT should yield `OK`, and ATI should yield a bunch of info:

```
Manufacturer: I: SAMSUNG
ELECTRONICS CO., LTD.
Model: I: SCH-R450/99
Revision: I: Q6055BSKAXLZ31501 1
[Nov 15 2007 24:00:00]
ESN: 0x[*FNORD*]
+GCAP: +CIS707-A, +MS, +ES, +DS,
+FCLASS

OK
```

If USB storage mode is enabled, you will probably also see an initDevice failed message. This is harmless, and the device will be recognized once you hit Done on the phone. Open System Preferences and go to Network. A box should pop up saying it found a new device, "Samsung CDMA Technologies". Choose it in the Show: dropdown box, and you'll get a modem settings page.

Set the account name to your phone number, `3055551234@mymetropcs.com`, and the password to mymetropcs. The telephone number is #777. Go to the Modem tab, and select Generic / Generic Dialup Device for the model. On 10.4, selecting "Verizon Support (PC 5220)" seems to work well.

If the phone likes the resulting init string and settings, you should be able to make the system dial it, and it'll almost immediately show an IP address in the 10.* range. You're in. Now you can immediately connect to anything, anywhere, on port 443.

MetroPCS blocks anything on ports other than 443. If you want Web access on 80, you're going to need to go through a proxy. They provide a web proxy at `wap.metropcs.com` port 3128. It doesn't appear to need a username/password. You can enter this in the Proxies tab under the network configuration. Entering it as a web http proxy works. I haven't been able to get other applications to connect through it properly if entered as a SOCKS proxy, so it may just be web only.

The wap.metropcs.com proxy is a strange one. It's got a captive portal, which is that same lovely semi-useless orange and blue "Downloads" page you get on the phone when you start the browser. After about a minute of inactivity, you get thrown back to that page with the next http request. If you hit that page from a normal web browser, you get a 404 thrown off from Apache Coccoon.

The `wap.metropcs.com` proxy also tends to be pretty slow, so you may want to find another proxy somewhere that listens on 443. A test run at speedtest.net through the Metro proxy showed 112 kbit/sec down, and 64 kbit/sec up, with a ping response of 999 msec. This isn't exactly EV-DO, but it isn't too bad either. I've found that FreeNX runs well over the connection to a ssh server on port 443 to connect up with a remote X11 desktop.

Windows users can also do this with a driver included in Samsung PC Studio. PC Studio won't do anything with the phone itself, but it'll drop the proper driver on the system for the "Samsung CDMA Technologies" device to use it as a modem.

Unfortunately, the phone software does not support Bluetooth dialup, so you're going to need the cable. The cable appears to just be a mechanical cable with no converters or anything.

For more information on the hidden features of the SCH-R450, check out the Samsung R450 Hacker's Manual, available on `handsonforums.com`.

For best results on the MetroPCS network, keep your phone's PRL up to date. Dial *228, wait for it to ask you what you're calling about, hit 2 and enjoy the wonderful little beat it plays. You should see "Programming in progress", "SPC Unlocked OK!", and "PRL Download OK!" appear on the bottom of the screen in a tiny font. When it finishes, it will reboot.

Enjoy, and happy hacking.

Shouts out to: Robert, who first introduced me to MetroPCS; Nikola Tesla and Guglielmo Marconi, who pioneered wireless transmission and telegraphy so many years ago, bringing us easy access to information today.

"Borrowing" the CustomInk.com Vector Library

by GantMan

If you've never used CustomInk.com, you're missing out on one of the coolest online shirt design companies of the past half decade. If you want to see what I'm talking about, go to CustomInk.com, click the tab at the top that says "The Lab", and then click on the left side to add art. You may notice that they have over 10,000 images you can add to your shirt, and they are scalable vector .EPS files that are dynamically loaded. The web is filled with people selling "vector packs" of basically scalable clipart that you can buy, but when you apply that math to number of clipart images CustomInk.com has, it's hard not to be wowed by the cost of such a library.

Evil cogs start a-turnin'. If this is dynamically loading the .EPS files into Flash for the shirt designer... shouldn't I be able to get some of those .EPS files for my own personal needs? Wouldn't it be nice to have the entire 10,000+ vector library for your own designs outside of the shirts? Or just for making a nice torrent for all your friends?

I was on Windows, so I began the adventure by loading up Fiddler (`http://www.fiddlertool.com/fiddler/`) and watching the HTTP requests. (Side note: I *love* Wireshark, but Fiddler is just better because it *only* listens to Internet Explorer. This allows you to have all your fun apps running, and even still browse the web in Firefox etc, without mucking up your packet captures. For anything that's not web related I load up Wireshark... and turn off just about every other application I have running, because I suck at Wireshark filters. :D)

Now that Fiddler was listening to IE, I pulled up the library from CustomInk. As the system loaded the images, it was pulling gifs from */clipart/gif/* So for example, one gif was from */clipart/gif/64772.EPS.gif* If you look at this path, it's easy to notice it's got a gif directory, and the gif already has the .EPS name. A simple, quick guess was that the .EPS was in an /eps/ directory with the normal .EPS extention. Using the above gif I generated the following guess and slammed it in the browser.

```
http://www.customink.com/clipart/
➥eps/64772.EPS
```

BOOYA! It gave me a download of a .EPS file. I opened it to find the delicious vector representation of the GIF I was just ogling. I typed in a few more, just to be sure, and everything came back perfect. So, one process I have is to go around and view all the GIFs and capture them all in Fiddler, press Ctrl + U to copy the URLs, do find and replace and pull down all those .EPS files. *But* the file names are sequential... so I can simply generate a list of URLs without any effort at all!

So now I needed to generate a bunch of sequential URLs. From my browsing, the eps files went from 10000.EPS to < 80000.EPS. Building a sequential text file would be easy. I chose to generate a quick VB script, since I was on a Windows machine at the time. I created a .VBS file on the desktop and inserted the code below:

```
Set fs = CreateObject("Scripting.
➥FileSystemObject")
Set a = fs.CreateTextFile("ALLEPS.
➥txt", True)
For xcount = 10000 TO 80000
     a.WriteLine("http://www.
➥customink.com/clipart/eps/" &
➥ xcount & ".EPS")
Next
a.Close
msgbox "Dun"
```

Running this .vbs file will put a file in the same directory, called ALLEPS.txt, with a bunch of generated URLs that should download CustomInk's .EPS library. Most of you know what to do with such a file, but, for the rest, you should download an application called "wget" for Windows (`http://gnuwin32.sourceforge.net/packages/wget.htm`). Wget is an app that comes from our *NIX friends, to "get" files from the web. Once I installed wget on the Windoze computer I was using, I ran the following command with a copy of the ALLEPS.txt file in the same directory:

```
wget --input-file=ALLEPS.txt
➥ --tries=2 --retry-connrefused
➥ -nc --waitretry=1 -v
```

This basically says, "gimme all the URLs from the file, try twice at most, and give it a second between each failed attempt."

After running the command and seeing file after file get pulled happily into my folder, I went to sleep. I awoke the following morning with the entire library :D

This isn't very nice to the CustomInk.com servers (about 10GB of vector files), so if you decide to design any shirts in the near future, please use their service so that they can pay their bills.

Hacking Your Hospital Bed

by The Piano Guy

Having recently been a multi-day guest of a local hospital, I was left to wait when it was time to check out. The beds were nice enough. They moved all the ways one would expect, the TV worked, they had a control panel for turning on and off the room lights and an emergency call button. All the typical stuff.

I did get roomed with a guy during my stay, however, and that made me wonder about the bed. He was agitated and more than a bit senile. Every time he would try to get out of the bed, an alarm would go off and they would have to come in and try to secure him again. I didn't understand (at first) how that worked from a technical perspective, as there were no motion sensors in the room.

On the last day, I found out. I was being discharged, and left alone in the room with the bed. I noticed the sticker on the panel at the foot of the bed that said "for hospital staff use only." Now, if you want to attract the undivided attention of flies, get some dog poop. If you want to attract the undivided attention of a hacker, put a sticker on it that says "for staff use only."

The bed was a Stryker Secure II. Made in Michigan, this is a company that my lawyer has bought stock in, but I digress. Before I lifted the panel, I took a closer look and noted the light indicators on the panel. There was a power indicator, a bed motion locked indicator, a warning light about the brake not being set, and an indicator for "bed exit on." I opened the panel, and no locking mechanism or alarm went off.

The first button was siderail control lights. It was possible for the nurse to override whether or not the patient could turn on or off his or her own lights. No big deal. The next button, Bed Motion, prevented the bed from moving at all with one button. The next set of buttons locked out the individual siderail component movements. I had to keep my leg up. The hospital could have enforced that, but I was happy to be compliant.

The next set of buttons allowed the hospital to set the angles from their part of the bed. The doctors would use this now and again during my stay, but more fun to watch was when the housekeepers had to remake the bed. They would bring it up chest high to make the bed. I wish I could do that with my bed at home - no more bending over.

The bed doubles as a scale. This feature can also be leveraged to make sure that the patient doesn't get out of bed without notifying staff. Please don't hurt yourself, but if you're ever in the bed and you can disarm the alarm, you can get out of bed unnoticed.

As a scale, from playing with the menus, I was able to figure out that the weight can be charted and trended over time, and of course is available in pounds or kilograms. All the data of the bed displays on a little plasma display.

The day before I was discharged, they had to switch me to a different room (because of the agitated senile roommate). I understand that it would have been more fair for him to be moved, but it made more sense for me to move. When they move a patient like this, they should let them keep the same bed if possible. They wheeled my bed over, and forgot to lock it. I went to get on it, and it started sliding across the floor at a rather rapid pace, toward my new roommate. It was all I could do to stop the bed from pushing into his (through the curtain). At that point, I moved the bed back, found the brake pedal on the side of the bed, locked it, and was able to get onto the non-moving bed. Even though this bed weighed hundreds of pounds, it rolled very easily. Heaven forbid there should be a fire and a patient isn't ambulatory, I'm sure they could get them out of there quite fast.

The one mystery I didn't learn about the beds in my time there was how they communicated with the light in the wall and the TV. Since there is only the one power cable that connects the bed to the wall (that I could find), I have to assume that there must be an X10 control. I went to their website (`http://www.stryker.com/➥en-us/products/PatientHandlin➥gEMSandEvacuationEquipment/Beds/➥MedSurgBeds/SecureII/index.htm`) and didn't find anything about how to connect the bed to the rest of the control circuits.

While I hope you have no need for a hospital stay, if you do, hope that your hospital has Stryker beds - unless you're trying to get out undetected.

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $100 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, email us at happenings@2600.com or by snail mail at Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

October 23, 24, 25
ToorCon 11
San Diego Convention Center
San Diego, CA
www.toorcon.org

October 24
LugRadio
Newhampton Arts Centre
Wolverhampton, England
www.lugradio.org

October 30, 31
PhreakNic 13
Days Inn Stadium
Nashville, TN
www.phreaknic.info

December 3, 4, 5, 6
Roboexotica - Festival for Cocktail Robotics
Freiraum
Museumsquartier/quartier21
Vienna, Austria
www.roboexotica.org

December 27, 28, 29, 30
Chaos Communication Congress
Berliner Congress Center
Berlin, Germany
ccc.de

February 5, 6, 7
ShmooCon
Wardman Park Marriott
Washington DC
www.shmoocon.org

April 15, 16, 17, 18
Notacon 7
Wyndham Cleveland at Playhouse Square
Cleveland, OH
www.notacon.org

July 16, 17, 18
The Next HOPE
Hotel Pennsylvania
New York, NY
www.hope.net

If you're involved in a hacker event, please send information on it to us so that more people can get involved! Of course, if you wait until the last minute to announce where it's being held, there's not a lot we can do to help. But if you know where and when your event is happening and it's not one of those corporate things that cost hundreds or even thousands of dollars just to walk in the door, email us the details at happenings@2600.com.

Events

HACK AIDS! The RA 2009 conference in Oakland, November 6-8, 2009, is the first major meeting to challenge the HIV=AIDS dogma in years. Meet top scientists as well as HIV-positive people who've rejected their diagnosis and the drugs that go with them. Learn how social engineering can protect HIV-positive people, how the censorship of alternative viewpoints works in science, and how the Internet is revolutionizing the dissemination of scientific heresy. http://ra2009.org. Contact: info@ra2009.org.

THE NEXT HOPE. July 16, 17, 18, 2010, Hotel Pennsylvania, New York City. http://www.hope.net

For Sale

ART FOR THE HACKER WORLD! Show your guests your inner g33k! Don't commercialize your living area with mass produced garbage! These are two original pieces of artwork inspired by technology that the *2600* reader fellowship will love! Check out the easy-to-remember links below and order today! http://tinyurl.com/2600art1 http://tinyurl.com/2600art2

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v26no3" and get 10% off of your order.

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

BSODOMIZER. A small, battery-powered, mischievous electronic gadget that interfaces between a laptop or desktop and VGA monitor and flashes a fake BSOD (Blue Screen of Death) onto the monitor at random time intervals or when triggered by an infrared remote control. This will cause the user to become confused and turn off or reset his or her machine. Limited run of 100 fully-assembled units available. Fully open source - schematics, firmware, and technical design documentation online if you want to build your own instead of buying one. Go to www.bsodomizer.com

KINGPIN EMPIRE. Represent the underground in style. Proceeds donated to hacker and health charities. Buy gear. Support the cause. Go to www.kingpinempire.com.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

Help Wanted

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

COMEDIAN/CONTROVERSIAL AUTHOR/ACTIVIST SEEKS HACKER willing to teach in person in Los Angeles area in exchange for valuable signed lithograph, comics, etc. Gabriel, 149 S. Barrington Ave. #162, Los Angeles, CA 90049

Wanted

THE TOORCON FOUNDATION is an organization founded by ToorCon volunteers to help schools in undeveloped countries get computer hardware and to help fund development of open source projects. We have already accomplished our first goal of building a computer lab at Alpha Public School in New Delhi, India, and are looking for additional donations of old WORKING hardware and equipment to be refurbished for use in schools around the world. More information can be found at http://foundation.toorcon.org.

WANTED: Local *2600* readers in the Hamilton/Burlington area to start a local *2600* regular meeting group. Contact don@jadedtech.com.

WANTED: Remote access to Chicago area computer using Comcast for Internet browsing in order to show originating Comcast IP. Compensation negotiable. Email: IP_chicago@yahoo.com

Services

COMPUTER FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the constitutional right to a zealous defense, and backs up that belief by providing the highest quality computer forensics and e-discovery support for criminal defense attorneys. Our experts are cool under fire in a courtroom and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment and abuse, terrorism and more. Sensei forensic technologists all hold prestigious forensics certifications. Our principals, President Sharon Nelson and Vice President John Simek are co-authors of *The Electronic Evidence Handbook* (ABA 2006) and of hundreds of articles. They lecture throughout North America on computer forensics. For more information, call us at 703-359-0700 or e-mail us at sensei@senseient.com.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

SECURITY ASSESSMENT AND EXPLOITS. Independent hacker available for LEGAL contracts. Penetration testing networks and systems remotely. Enumeration of networks, systems, servers, VPNs, and cryptography. Identifying software vulnerabilities specific to web based applications and web facing operating systems as well as special requests. Full disclosure via professional detailed technical report. Inquiries to canada2600@gmail.com. Powered by http://www.canada2600.org

JEAH.NET UNIX SHELLS & HOSTING. JEAH is celebrating its 10-year anniversary as #1 for fast, stable, and secure UNIX shell accounts. Use hundreds of IRC vhost domains and access all shell programs and compilers. JEAH.NET also features rock-solid UNIX web hosting. *2600* readers' setup fees are always waived. We support *2600,* because we read too! Oh, and don't forget our private domain name registration at FYNE.COM.

KALETON INTERNET provides secure and private web hosting, domain name registrations, and email accounts. We have offshore servers, anonymous payment methods, and strongly support freedom of speech. Visit us at www.kaleton.com now to see how we can help you.

WWW.NAMETROLLEY.COM has affordable domain names, low cost web hosting plan with extensive language support, SSL Certificates, email accounts, free photo album, free blog, free forwarding and masking, complete DNS control, over 40 TLDs to choose from, 24/7 support, and much much more.

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law in Pennsylvania and New Jersey. Free consultation to *2600* readers. http://muentzlaw.com alex@muentzlaw.com (215) 806-4383

INFORMATION INJECTION is a new site that is designed to educate the masses. We all know that human stupidity is security's weakest link, so let's try a little education as the patch! http://infoinject.org for elites and newbs alike!

BANDIT DEFENSE: SECURITY FOR THE LITTLE GUY. I'll hack into your computer systems and then help you fix all the security holes. I specialize in working with small businesses and organizations, and I give priority to those facing government repression. My services include: hacking your organization from the Internet (comprehensive information gathering and reconnaissance, web application security testing, remote exploits), hacking your organization from your office (physical security, local network audits, and exploitation), wireless network security (slicing through WEP, brute forcing WPA), electronic security culture (evading surveillance, encryption technology, etc.), and other misc. services. More details at www.banditdefense.com, or email info@banditdefense.com.

INCARCERATED *2600* MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of www.BrazilBoycott.org, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one million neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

Announcements

JAVA PROGRAMMING BLOG. Visit http://enableassertions.blogspot.com. It is time to learn Java. Recent topics include puzzles, book reviews, code viewers, file parsing, exceptions, sorting, and constructors.

CHEER10S.COM. News Syndicate from the Underground! Posting original and reposted news about the hacking and phreaking world. Regularly posted and looking for news submissions from members. http://www.cheer10s.com

PUBLIC INTELLIGENCE IN THE PUBLIC INTEREST. Collect. Connect. Reconfigure. I live in NYC and work as Executive Director with HOPE's first ever speaker, Robert Steele, President for the 501c3, Earth Intelligence Network (www.earth-intelligence.net & twitter.com/earthintelnet & OSS.net). Our online public intelligence journal can be found at http://phibetaiota.net. Other related links: http://re-configure.org & http://smart-city.re-configure.org. Contact earthintelnet@gmail.com

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and Central America at 5110 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2008 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

Personals

LOOKING FOR HACKERS AND PHREAKERS! If interested email me at Albany2600@gmail.com

INTERESTED IN REAL WORLD HACKING: Looking to brainstorm via mail (for the incarcerated), email, instant messaging, and eventually over phone. Know anything about locks, safes, phone eavesdropping, scanners, or being in or at places when and where you don't belong? I want to talk real shop, trade ideas, thoughts, etc. Will communicate with all, including those down as I have been there seven straight. Contact info: HF, PO Box 320278, Cocoa Beach, FL 32932 - better yet, username Misterh083 on Yahoo IM, AOL IM, & gmail. Can you bypass Windows XP Pro admin password? Know phone boxes? Mycology? Thanks for reading. Shout out to Stormbringer - 083; keep your chin up.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Winter issue: 11/25/09.

CLUB-MATE®

The German beverage invasion continues and we're only too happy to help make it possible. As many of you know, Club Mate has proven to be extremely popular in the hacker community. First introduced in the United States at The Last HOPE in 2008, this caffeinated, carbonated, comparatively low in sugar drink has really taken off. Both HOPE attendees and German operatives tell us that one gets a burst of energy similar to all of those energy drinks that are out there without the "energy drink crash" that usually comes when you stop consuming them. Some people love the taste right away, others need a little convincing. As the Club Mate motto goes, "one gets used to it."

Over the summer, we've distributed Club Mate to various hacker spaces around the country and we also had a special "Club Mate Day" in the New York region where people had cases delivered to their homes in the *2600* phone company van! It was utter mayhem and a great time for all. Now we're ready to have cases delivered around the country as well as full pallets (800 half-liter bottles) at a steeply discounted rate (great for hacker spaces).

For full pricing and delivery info, visit club-mate.us and to make specific inquiries, email contact@club-mate.us.

"There is no need for any individual to have a computer in their home."
- Ken Olson, president, Digital Equipment Corp., 1977

Staff

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Redhackt

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Acidus, Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, Paul Estev, Mr. French, glutton, Javaman, Joe630, Graverose, Kingpin, Kn1ghtl0rd, Kevin Mitnick, OSIN, The Prophet, David Ruderman, Screamer Chaotix, Silent Switchman, StankDawg, Mr. Upsetter

Webmaster: Juintz

Network Operations: css

Broadcast Coordinators: Juintz, thal

IRC Admins: beave, mangala, koz, r0d3nt

Forum Admin: Skram

Inspirational Music: Hypernova, Arctic Monkeys, Diana Ross, Los Aterciopelados, Dobie Gray, PSB

Shout Outs: MC Manus, Shelly Stone, Jarlacher, The Rude Dude, Mograf, Apple V, phillyboombotz, MAD, Rob & Peg, Aldert, Koen, Kyle, h1kari, volt4ire, London 2600, the Dublin crew, the staff and attendees of ToorCamp and HAR

2600 *(ISSN 0749-3851, USPS # 003-176); Autumn 2009, Volume 26 Issue 3, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2008 at
$25 per year, $34 per year overseas
Individual issues available from 1988 on at
$6.25 each, $8.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

Copyright © 2009; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: The "Cruzat Beer House" bar, Sarmiento 1617 (first floor, Paseo La Plaza).

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the wi-fi hotspot. 6 pm

British Columbia

Kamloops: Old Main Building coffee shop in front of the registrar's office on Student Street, TRU Campus.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center Food Court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Kildare House, 1880 Wyandotte St E. 7 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Grove Inn. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Borders entrance to Chapelfield Mall. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm

Paris: E-Dune bar, 18 Ave Claude Vellefaux. 6 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

Rouen: Place de la Cathedrale by the benches in front. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food Court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Unlimited Coffee, 741 E. Glendale Ave. 6 pm.

Prescott: Barnes and Noble cafe in the Prescott Gateway Mall.

Arkansas

Ft. Smith: Sweetbay Coffee, 7908 Rogers Ave. 6 pm

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

Connecticut

Newington: Panera Bread on the Berlin Turnpike. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St. (in Pentagon Row on the courtyard) 7 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Fashion Square Mall food court, 2nd floor.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Mercury Cafe, 1505 W Chicago Ave.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown at 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Marlborough: Solomon Park Mall food court. 6 pm

Northampton: Downstairs of Haymarket Cafe. 6 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University.

Minnesota

Minneapolis: Java J's coffee house, 700 N Washington.

Missouri

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

Omaha: Westroads Mall southern food court, 100th and Dodge. 7 pm

Nevada

Las Vegas: reJAVAnate Coffee, 3300 E Flamingo Rd (at Pecos). 7 pm

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. 5:30 pm

New York

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Panera Bread, 2373 W Ridge Rd. 7:30 pm

North Carolina

Charlotte: Panera Bread Company, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: The Brew House, 1047 E McMillan. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm.

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas by Borders on first floor.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Lane, outside porch near the entrance. 7:30 pm

Houston: Ninfa's Express next to Nordstrom's in the Galleria Mall. 6 pm

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm.

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Unusual Looking Payphones

France. The unusual thing about this phone found in the countryside is the fact that it takes neither coins nor cards. In fact, this phone can only make emergency calls or calls using credit or calling cards. In France, the law states that every city, town, or village must have at least one payphone.

Photo by Mike Miller

Japan. They don't really get much pinker than this model, found in a park in Ueno, Tokyo.

Photo by Jim E. Etheredge II

Thailand. Seen in a place called Chiang Mai, or perhaps it was just a hallucination.

Photo by professor ned

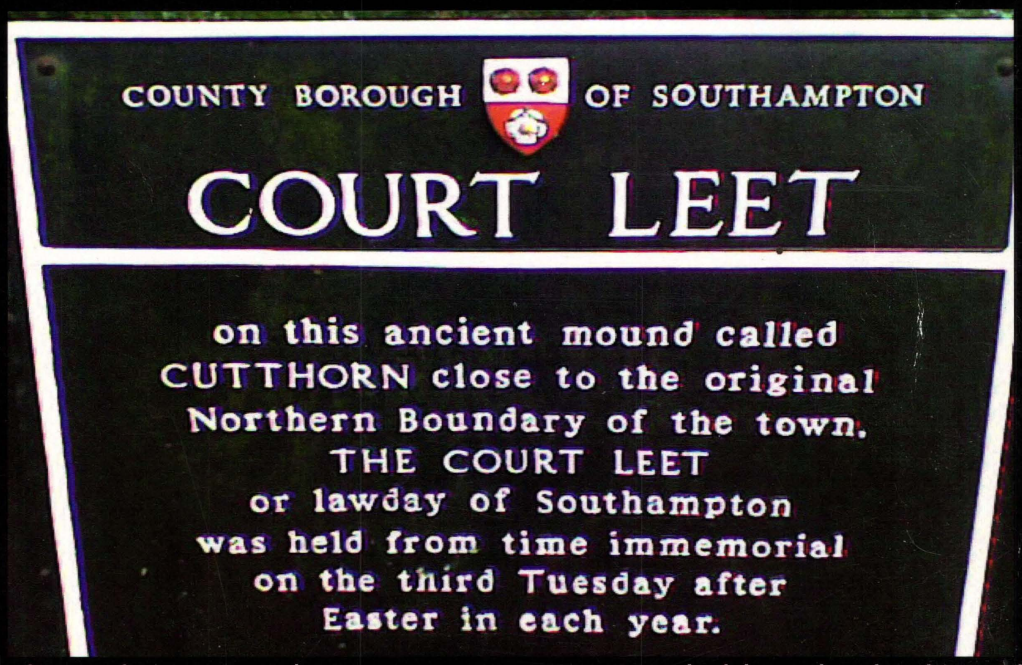
Russia. This was actually the grand opening of a payphone in Kamchatka Oblast. We can't even imagine one of our phones being celebrated so festively. These people must really appreciate telephony.

Photo by Curtis Vaughan

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
Email your submissions to payphones@2600.com.
Do not send us links as photos must be previously unpublished.

The Back Cover Photos

Now here's a campaign we can all get behind. This race took place in Illinois and we don't really know how it turned out. But that's not the point, is it? Thanks to **Rich Tordia** for letting us know about our increasing political presence.


COUNTY BOROUGH OF SOUTHAMPTON
COURT LEET
on this ancient mound called
CUTTHORN close to the original
Northern Boundary of the town.
THE COURT LEET
or lawday of Southampton
was held from time immemorial
on the third Tuesday after
Easter in each year.

Perhaps this is the true predecessor to *2600* meetings held on the third Tuesday after Easter. Thanks to **Mr. Skillz** for letting us know how elite things once were back in the medieval days.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).